Online ISSN : 0975-4172
Print ISSN : 0975-4350

Global Journal

of Computer Science and Technology: E

Network, Web & Security

Highlights

Novel Approach to Compute

Metrics for Quality Assurance

Security Issues and Energy

Performance Evaluation and QoS

Discovering Thoughts, Inventing Future

VOLUME 15 ISSUE 7 VERSION 1.0

Global Journal of Computer Science and Technology: E
Network, Web & Security

Global Journal of Computer Science and Technology: E
Network, Web & Security

Volume 15 Issue 7 (Ver. 1.0)

Open Association of Research Society

The opinions and statements made in this book are those of the authors concerned. Ultraculture has not verified and neither confirms nor denies any of the foregoing and no warranty or fitness is implied.

Engage with the contents herein at your own risk.

The use of this journal, and the terms and conditions for our providing information, is governed by our Disclaimer, Terms and Conditions and Privacy Policy given on our website http://globaljournals.us/terms-and-condition/ menu-id-1463/

By referring / using / reading / any type of association / referencing this journal, this signifies and you acknowledge that you have read them and that you accept and will be bound by the terms thereof.

All information, journals, this journal, activities undertaken, materials, services and our website, terms and conditions, privacy policy, and this journal is subject to change anytime without any prior notice.

Incorporation No.: 0423089
License No.: 42125/022010/1186
Registration No.: 430374
Import-Export Code: 1109007027
Employer Identification Number (EIN):
USA Tax ID: 98-0673427

Global Journals Inc.

*(A Delaware USA Incorporation with "Good Standing"; **Reg. Number: 0423089**)*

Sponsors: Open Association of Research Society
Open Scientific Standards

Publisher's Headquarters office

Global Journals Headquarters
301st Edgewater Place Suite, 100 Edgewater Dr.-Pl,
Wakefield MASSACHUSETTS, Pin: 01880,
United States of America
USA Toll Free: +001-888-839-7392
USA Toll Free Fax: +001-888-839-7392

Offset Typesetting

Global Journals Incorporated
2nd, Lansdowne, Lansdowne Rd., Croydon-Surrey,
Pin: CR9 2ER, United Kingdom

Packaging & Continental Dispatching

Global Journals
E-3130 Sudama Nagar, Near Gopur Square,
Indore, M.P., Pin:452009, India

Find a correspondence nodal officer near you

To find nodal officer of your country, please email us at *local@globaljournals.org*

eContacts

Press Inquiries: *press@globaljournals.org*
Investor Inquiries: *investors@globaljournals.org*
Technical Support: *technology@globaljournals.org*
Media & Releases: *media@globaljournals.org*

Pricing (Including by Air Parcel Charges):

For Authors:

22 USD (B/W) & 50 USD (Color)

Yearly Subscription (Personal & Institutional):
200 USD (B/W) & 250 USD (Color)

Integrated Editorial Board (Computer Science, Engineering, Medical, Management, Natural Science, Social Science)

President Editor (HON.)

Chief Author (HON.)

Dean & Editor-in-Chief (HON.)

Contents of the Issue

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 15 Issue 7 Version 1.0 Year 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

A Novel Approach to Compute the Handover Probabilities based on Mobility in WPAN

By Ch.Subrahmanyam & K. Channakesavareddy
ECE at Jawaharlal Nehru Technological University, India

Abstract- A novel approach has been presented to compute the probabilities of unsuccessful handovers based number of free channels available in the target AP and number of free channels available plus based on the mobility of mobile device. The number of free channels in the AP is 16 and the mobility of the mobile device in the 8 different directions is considered. The directions of movement are 0, 45, 90, 135, 180, 215, 270 and 315 that a mobile can take a turn to. If the mobile device is handed over to the target AP based on the movement of the mobile device, then the proposed model can be used to compute the probabilities of the unsuccessful handover if the number of free channels in the target AP is different than expected with respect to the host AP. The probabilities of the incorrect decision is plotted for the cases of mobile device moving in a direction normal to the boundary and moving along the boundary are plotted.

Index Terms: *unsuccessful handovers, wpan probability modeling, decision time, mobility.*

GJCST-E Classification : *C.1.3 C.1.4*

A Novel Approach to Compute the Handover Probabilities based on Mobility in WPAN

Ch.Subrahmanyam [α] & K. Channakesavareddy [σ]

Abstract- A novel approach has been presented to compute the probabilities of unsuccessful handovers based number of free channels available in the target AP and number of free channels available plus based on the mobility of mobile device. The number of free channels in the AP is 16 and the mobility of the mobile device in the 8 different directions is considered. The directions of movement are 0, 45, 90, 135, 180, 215, 270 and 315 that a mobile can take a turn to. If the mobile device is handed over to the target AP based on the movement of the mobile device, then the proposed model can be used to compute the probabilities of the unsuccessful handover if the number of free channels in the target AP is different than expected with respect to the host AP. The probabilities of the incorrect decision is plotted for the cases of mobile device moving in a direction normal to the boundary and moving along the boundary are plotted.

Index Terms: unsuccessful handovers, wpan probability modeling, decision time, mobility.

I. Introduction

Mobility of the mobile devices plays an important role in the handover. When the mobile devices are stationary with respect to the access points (AP), then it is easy for the network to decide where the mobile device needed to be handed over to. For example, the mobile devices can be handed over to the nearest AP. Again the handover is based on several criteria like available bandwidth [1], received signal strength [2,3], Bit error rate, mobility etc[4]. Handovers based on the mobility are very important compared to all other parameters. The mobility based handovers are very popular in the wireless networks [4]. The mobility may be defined as the movement of the mobile device in a certain direction and the handover is initiated based on the location of the mobile device after certain interval of time. It may be possible that handover is initiated assuming that the mobile device will be there in the service zone of the next AP, but eventually the mobile device will not arrive into that service zone since mobile device has changed the direction of its movement in the mean time.

Mobility based handovers were analyzed by some researchers [4] for the wireless communications. The performances of various algorithms were discussed in ref [5]. A survey was conducted by Camp et.al on the subject of the mobility based handovers in the wireless networks [6]. Vijayan et.al developed models to compare the performance of the handover algorithms [5]. However there was a limitation in this approach that the model has limited application to heterogeneous networks.

The problem of type network such as homogenous, heterogeneous, horizontal or vertical networks was overcome by the model proposed by Chi .et. al [1]. The unsuccessful handover were analyzed by the Chi et.al for the two node wireless network models, but based on the band width. Authors have extended the models to a generalized model for 2, 3, 4 and 5 node networks for WPAN/WLAN environment [7]. It was discussed in [7] about how the unsuccessful handover probability models can be extended to the WPAN/WLAN environment. Also a common approach has been proposed in [7] on how to select a set of APs depending up on the location of the mobile device.

Akhila et. al [3,4] developed a model for the handovers in the wireless environment. However, the model proposed by Akhila et.al focused on the handovers based on mobility only [4]. It did not focus on the combined effect of mobility and the band width together, since, if the handover is initiated based on the direction of movement, and enough bandwidth is not available when the actual transfer happens in the target AP, then it becomes an unsuccessful handover. In this work, a generalized handover model that was developed as part of the work by authors [7] is extended to mobility based handover also. That is, the proposed model considers 2-AP, 3-AP, 4-AP and 5-AP models, with free bandwidth and with free bandwidth plus mobility. This model is more realistic for hospital environment as the proposed model involves WPAN application, different AP models, fee channels and mobility based handovers. Other handover algorithms are developed by various researchers that can be found in [8-12].

In Sec.II, physical model and handover approach in a hospital environment has been developed. In Sec.III, the generalized probability model that has been developed in [7] is extended to consider the mobility also. In Sec IV, the models were run and simulation results are discussed for 2-AP, 3-AP, 4-AP and 5-AP models by solving the probabilities equations presented in Sec. III. The results are presented two cases, when the mobile device was moving normal to

Author α : Dept. of ECE at Jawaharlal Nehru Technological University, Hyderabad. e-mail: subbunvl@yahoo.com
Author σ : Professor from ECE Dept., Jawaharlal Nehru Technological University, Hyderabad). e-mail: kesavary@rediffmail.com

the boundary and when it was moving along the boundary. The probabilities of unsuccessful handover that has happened unnecessarily, probability of handover that has missed to happen and total probability of unsuccessful handover due to incorrect decision are presented for the two cases. Finally, important conclusions are drawn in Conclusions section.

II. Physical Model and Handover Approach

Fig.1 shows a hospital that has several rooms open to the hall area. There is room dedicated for parking the mobile devices that are used for the diagnosis. Also there are other mobile devices in the hall area that are not necessarily used for diagnosis, but devices like laptops, tablets etc. Hence all of these devices along with the diagnosis devices are treated as mobile devices. The devices used for diagnosis purpose are parked in the parking in room when not being used. Also, these devices are electrically charged when they are parked in the parking room. Fig.1 shows the mobile device M1 moving from the Parking Room to Patient Room 2. When M1 is the service zone of AP-NE, the M1 is served by that AP. But when the M1 is crossing the boundary, then the M1 has to be serviced by the nearest AP. For example when the M1 enters the service zone of AP-NW, then it is served by that AP.

Assume that AP-NE has sufficient number of free channels and it is serving M1, then it also understands that the M1 is moving a specific speed and moving towards the AP-NW service zone. This is understood by the AP-NE, by exchanging the singles frequently with M1. By getting the time interval of the received signals from M1, the AP-NE calculates the location coordinates of M1, direction of movement as well as its speed of movement. Based on the speed of movement and direction of movement, AP-NE initiates a hand over of M1 to AP-NW when it is at the boundary of the AP-NE service zone. The handover may be treated as successful if AP-NW has sufficient number of free channels as well as the number of free channels in the AP-NW is higher than the AP-NE. If the number of free channels in AP-NW is less than the AP-NE, the handover is considered as unsuccessful. If the AP-NW does not have any free channels at all when the handover takes place, the M1 is becomes an orphan node and the connection is lost. This is known as unsuccessful handover that happened unnecessarily. The AP-NE might have continued to serve the M1 while it is in AP-NW zone since the number of free channels in AP-NE is more than that of AP-NE.

Other possibility is, when the decision is taken to handover the M1, the AP-NE checks the number of free channels available in AP-NW. if the number of free channels in AP-NW is less than that in AP-NE, the AP-NE does not handover the M1 to AP-NW, but, M1 continues to move into the AP-NW zone.

The M1 moves from parking room (AP-NE zone) to patient room 2 (AP-NW zone). Then from patient room 2 to radiology lab 1, that is from AP-NW zone through AP-C zone to AP-NE zone. Path 3 shows the M1 moving from radiology lab 2 to ICU-1 and then from ICU-1 to parking room. Depending upon the location of the mobile device, there is possibility of handover taking place to the nearest access point. The AP model to be chosen for handover is given in ref [7].

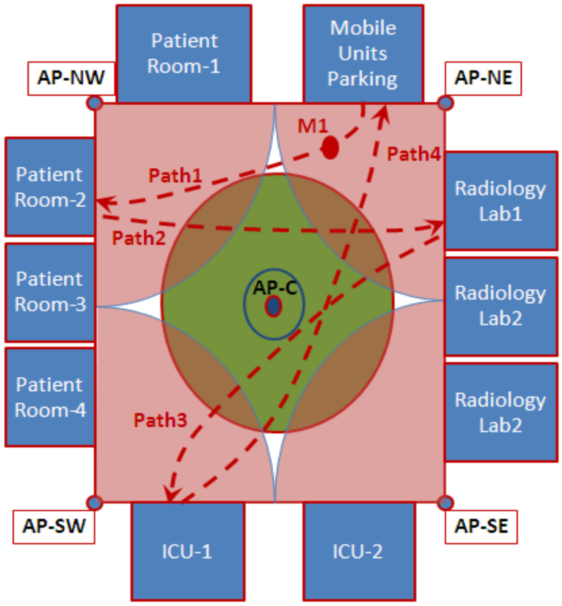


Figure 1 : A hospital hall area with a mobile device M1 moving around the hall

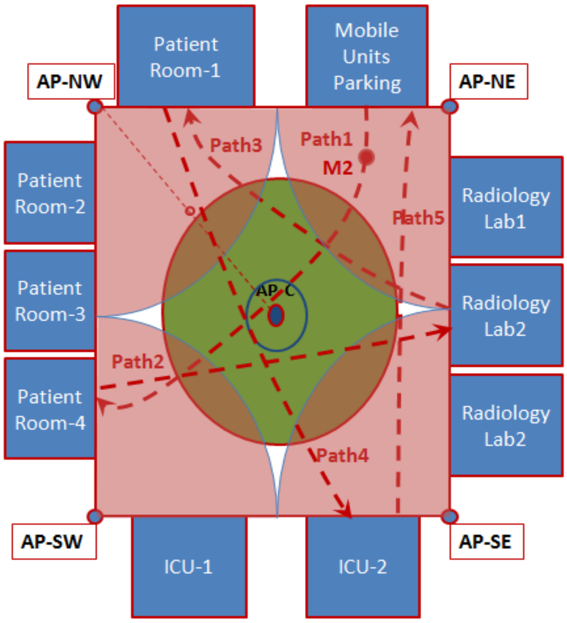


Figure 2 : A hospital hall area with a mobile device M2 moving around the hall

Fig. 2 shows another case of the paths followed by the mobile device M2. In this case, when path 5 is carefully observed, the path 5 is almost tangential to the service zone of AP-C. If the handover happens to AP-C from AP-SE, then it is a handover that happened unnecessarily. But f is just inside the AP-C zone, then another handover has to happen immediately since the M2 is moving to the zone of AP-NE. Hence based on the speed and direction of movement, the handover can be delayed to prevent handovers happening unnecessarily.

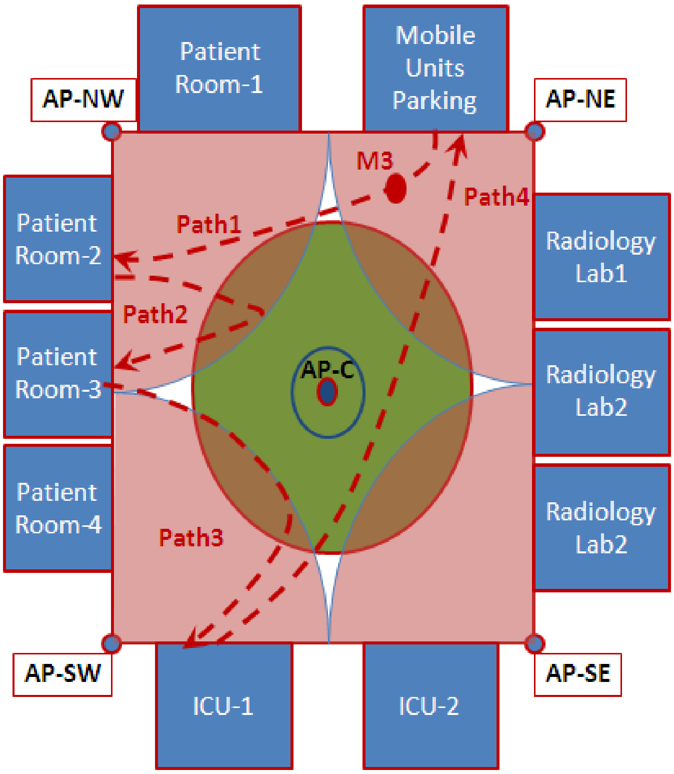


Figure 3 : A hospital hall area with a mobile device M3 moving around the hall

Fig.3 shows the movement of mobile device M3 in 4 paths. Path 2hsoews that M2 moved from patient room 2 towards the boundary of the AP-NW. Based on the direction and speed of movement, the handover happens from AP-NW to AP-C. But it changes its direction back into the AP-NW zone without actual crossing into AP-C. Hence the handover happened here again unnecessarily. A slight delay in decision making would bring reduction in unnecessary handovers, in this case also.

Path3 is very peculiar since the movement is along the boundary of the AP-SW zone. Here depending up on the location of M3 with respect to the boundary, the M3 can be either in AP-SW zone or in AP-C zone or it can move back and forth into and out of these two zones. Hence the handover has to happen frequently when M3 is moving along this path.

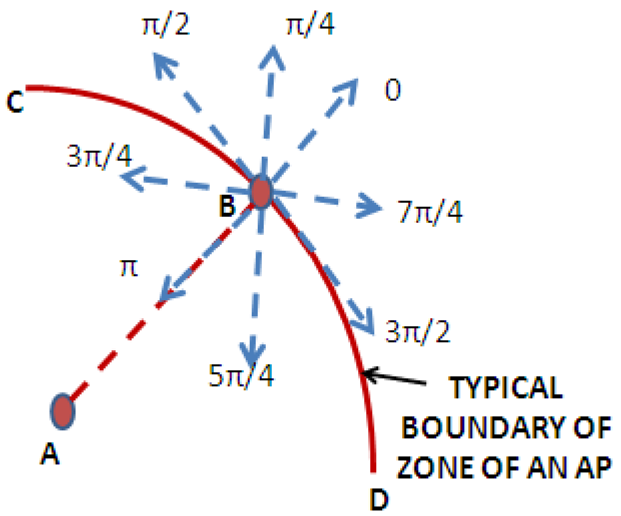


Figure 4 : Movement vectors with respect to a typical boundary when mobile device moving normal to the boundary

III. Probability Model

Fig. 4 shows the vectors representing the direction of the movement. Initially the mobile device is inside the service zone is at point A and then starts moving towards point B. The arc CBD represents a typical boundary of the service zone of an AP. When the mobile device is inside the arc CBD, then the AP serves the mobile device. When it is outside the arc CBD, then the mobile device is served by another nearest AP after successful handover. In Fig.4, relative vectors shown at point B. The mobile device that has reached point B can continue its movement in the same direction which is 0radians. The angles are defined with respect to its present movement. The mobile device can take left turns at $\pi/4$ or $\pi/2$. Or it can take the right turns at $3\pi/2$ or $7\pi/4$. In all these cases of 0˒ $\pi/4$, $\pi/2$, $3\pi/2$ or $7\pi/4$ the mobile node location is outside the arc CBD, and hence needed to be handed over to the nearest AP. If the mobile device takes turns at angles $3\pi/4$, π or $5\pi/4$, the mobile device needed to be retained with the same AP. The probabilities of the mobile device moving in the directions of angle

$$P_{\theta_i} = P_0 \frac{1}{\sigma_{\theta_i}\sqrt{2\pi}} e^{\frac{\theta_i^{\,2}}{2\sigma^2{}_\theta}} + P_{\pi/4} \frac{1}{\sigma_{\theta_i}\sqrt{2\pi}} e^{\frac{\left(\theta_i - \frac{\pi}{4}\right)^2}{2\sigma^2{}_\theta}} +$$

$$P_{\pi/2} \frac{1}{\sigma_{\theta_i}\sqrt{2\pi}} e^{\frac{\left(\theta_i - \frac{\pi}{2}\right)^2}{2\sigma^2{}_\theta}} + P_{3\pi/4} \frac{1}{\sigma_{\theta_i}\sqrt{2\pi}} e^{\frac{\left(\theta_i - \frac{3\pi}{4}\right)^2}{2\sigma^2{}_\theta}}$$

$$+P_{\pi}\frac{1}{\sigma_{\theta_i}\sqrt{2\pi}}e^{\frac{(\theta_i-\pi)^2}{2\sigma^2{}_{\theta}}}+P_{5\pi/4}\frac{1}{\sigma_{\theta_i}\sqrt{2\pi}}e^{\frac{\left(\theta_i-\frac{5\pi}{4}\right)^2}{2\sigma^2{}_{\theta}}}$$

$$+_{3\pi/2}\frac{1}{\sigma_{\theta_i}\sqrt{2\pi}}e^{\frac{\left(\theta_i-\frac{3\pi}{2}\right)^2}{2\sigma^2{}_{\theta}}}+P_{7\pi/4}\frac{1}{\sigma_{\theta_i}\sqrt{2\pi}}e^{\frac{\left(\theta_i-\frac{7\pi}{4}\right)^2}{2\sigma^2{}_{\theta}}} \tag{1}$$

Where P_{θ_i} the relative is change in direction at the junction and $P_{\pi/4}$ are the probabilities of the mobile device moving in the direction of π/4. $P_{\pi/4}$ is obtained from the historical data. When a Mobile device is on the arc CBD, handover is initiated assuming that the Mobile device will enter into the service zone of the next available nearest APs. But if it does not move into that zone, then the handover has happened unnecessarily. Therefore the probability of the handover that has happened unnecessarily is given by

$$P_{hu-mob}=P\left(\frac{3\pi}{4}\right)+P(\pi)+P\left(\frac{5\pi}{4}\right) \tag{2}$$

When a Mobile device is just inside or on the arc CBD, handover is not initiated assuming that the Mobile device will remain in the service zone of the same AP. But if it moves into the next zone during the decision time, then the handover has missed to happen. Therefore the probability of the handover that has missed to happen is given by

$$P_{hm-mob}=P\left(\frac{3\pi}{2}\right)+P\left(\frac{7\pi}{4}\right)+P(0)+P\left(\frac{\pi}{4}\right)+P\left(\frac{\pi}{2}\right) \tag{3}$$

Similarly when the mobile device is initially at point D and is moving along the arc DBC towards point B. At point B, the mobile device can take a turn into any of the eight available turns. Handover is initiated assuming that the mobile device is moved into any of the turns at 0' 7π/4, 3π/2, 5π/4 or π while it actually takes a turn to any of the angles π/4, π/2, or 3π/4. Then the handover happens unnecessarily. Therefore the probability of the handover that has happened unnecessarily is given by

$$P_{hu-mob}=P\left(\frac{\pi}{4}\right)+P\left(\frac{\pi}{2}\right)+P\left(\frac{3\pi}{4}\right) \tag{4}$$

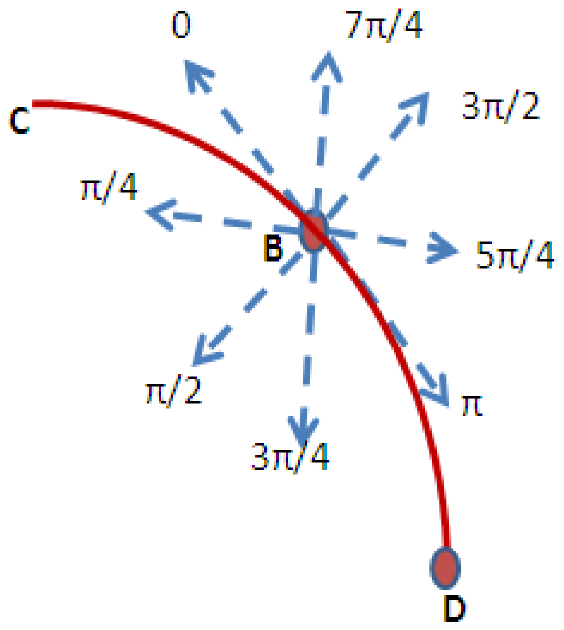


Figure 5 : Movement vectors with respect to a typical boundary when mobile device moving along the boundary

If handover is not initiated assuming that the mobile device is moved into any of the turns at π/4, π/2, or 3π/4 while it actually takes a turn to any of the angles 0' 7π/4, 3π/2, 5π/4 or π. Then the handover has missed to happen. Therefore the probability of the handover that has missed to is given by

$$P_{hm-mob}=P(0)+P\left(\frac{7\pi}{4}\right)+P\left(\frac{3\pi}{2}\right)+P\left(\frac{5\pi}{4}\right)+P(\pi) \tag{5}$$

The probability of handover that happened unnecessarily and that has missed to happen based on the availability of free channels in the target AP are given by

$$P_{hu-chn}=\sum_{i=1}^{n}\sum_{\substack{j=1\\ j\neq i}}^{n}P_iP_{j/i}\sum_{m=X}^{A_j}\Pi_{j,A_j-m}\sum_{k=0}^{m-X}\Pi_{i,A_i-k}\Omega_i(k,r,t)$$

$$\bullet\sum_{n=0}^{A_i}\Pi_{i,A_i-n}\sum_{k=n+X}^{A_j}\Pi_{j,A_j-k}\Phi_j(k,r,t)$$

$$P_{hm-chn}=\sum_{i=1}^{n}\sum_{\substack{j=1\\ j\neq i}}^{n}P_i\left(1-P_{j/i}\right)\sum_{n=0}^{A_i}\Pi_{i,A_i-n}\sum_{k=0}^{n+X-1}\Pi_{j,A_j-k}\Omega_j(k,r,t)$$

$$\bullet\sum_{m=X-1}^{A_J}\Pi_{j,A_j-m}\sum_{k=m-X+1}^{A_i}\Pi_{i,A_i-k}\Phi_i(k,r,t) \tag{6}$$

Refer to [1,7] for more details about the nomenclature and details about the above two equations.

The total probability of the handover that happened unnecessarily, since the mobile device has been transferred to the next available AP based on the movement of the mobile device, but the number of free channels in the present AP is higher than that in the target AP when the actual transfer happens. Therefore,

$$P_{hu} = P_{hu-mob} * P_{hu-chn} \tag{7}$$

Similarly,

The total probability of the handover that has missed to happen is

$$P_{hm} = P_{hm-mob} * P_{hm-chn} \tag{8}$$

The unsuccessful handover probability due to incorrect decision is given by

$$P_{ush} = P_{hu} + P_{hm} \tag{9}$$

IV. Simulation Results

In this work, simulations are run for the cases of handover probabilities when only bandwidths are considered as criteria for handovers, and bandwidths plus movement of the mobile device are considered as criteria for the handover. Table 1 shows the probabilities for four different case. Each case shows the probabilities for the mobile device moving in certain angles. These probabilities are assumed here for the simulation purpose. However, these probabilities are to be derived from the historical data for each application like hospitals, railway stations, bus stations etc. In case 1, there is probability of 0.1 that a mobile device moves in the same direction (0 degrees). That means, 1 out of 10 mobile devices always moves in the same direction of its approach. Another probability of 0.3 exists at 135 degrees. Similarly there are probabilities defined for 8 different angles for each of four cases.

Table 1: Probabilities of Mobile device taking a turn

	Case 1	Case 2	Case 3	Case 4
P0	0.1	0.5	0.02	0.04
Pπ/4	0.08	0.02	0.06	0.09
Pπ/2	0.05	0.1	0.09	0.02
P3π/4	0.3	0.2	0.4	0.03
Pπ	0.1	0.04	0.1	0.2
P5π/4	0.2	0.09	0.03	0.02
P3π/2	0.08	0.02	0.2	0.1
P7π/4	0.09	0.03	0.1	0.5

Table 2 shows the probabilities that handover happened unnecessarily and that has missed to happen for the cases when the mobile device was moving towards the boundary of the service zone and when the mobile device was moving along the boundary. These probabilities are obtained after solving the equations listed in the last section.

Table 2 : Computed unsuccessful probabilities when handover happened unnecessarily and when handover missed to have happened

	Normal to Boundary		Along Boundary	
	Phu	Phm	Phu	Phm
Case 1	0.4457	0.2538	0.44	0.2493
Case 2	0.4644	0.591	0.5129	0.4134
Case 3	0.3451	0.3641	0.4042	0.1554
Case 4	0.5015	0.4016	0.4566	0.6028

Fig. 6 shows the probability of the handover that has happened unnecessarily for cases with only free channel; and free channel plus mobility care considered as criteria, when the mobile node was moving in the normal direction to the boundary of the service zone and for the case 1 scenario. The 4 different models of 2-AP, 3-AP, 4-AP and 5-AP are run. 2-AP-Chn model is the one where the 2-AP model with free channel availability is considered for the handover criteria. 2-AP-Chn-Mob is the one where the 2-AP model with free channel availability and mobility is considered for the handover criteria. Similarly other models are named in Fig. 6 to 11.

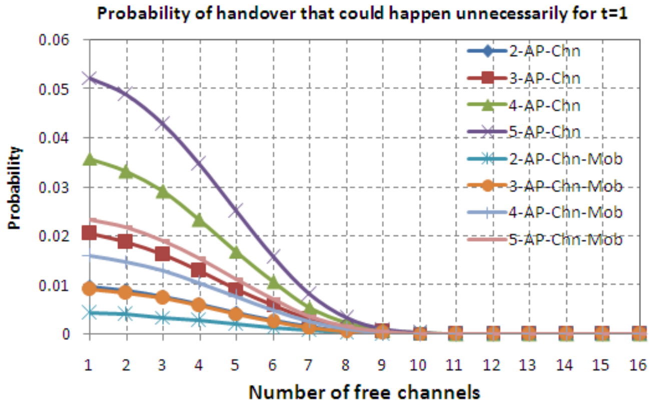


Figure 6 : Probability of the handover that has happened unnecessarily for cases with only free channel and free channel plus mobility considered as criteria

From Fig. 6, it shows that when there is 1 free channel, the unsuccessful handover probability is 5.2% for the 5-AP-Chn model, and it is 2.4% for 5-AP-Chn-Mob model. The probabilities are reduced by 50% when the mobility models are considered. 4-AP-Chn model yielded 3.5% of unsuccessful handover probability that has happened unnecessarily, where as it is 1.6% in 4-AP-Chn-Mob model when the number of free channels available is just one in the target AP.

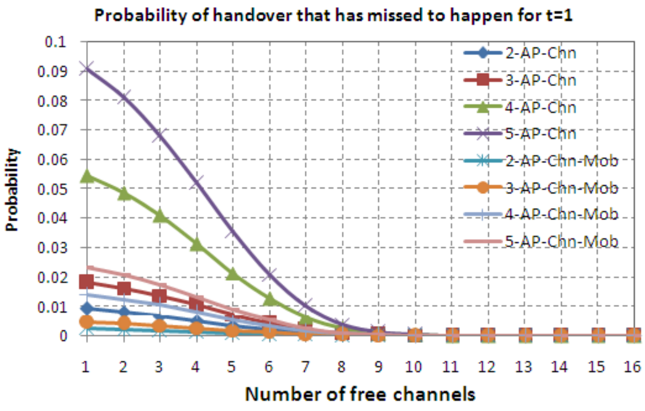


Figure 7 : Probability of the handover that has missed to happen for cases with only free channel and free channel plus mobility considered as criteria

Fig. 7 shows the probability of the handover that has missed to happen. It is clear from Fig.7 that when there is 1 free channel, the unsuccessful handover probability is 1% for the 2-AP-Chn model, and it is 0.3% for 2-AP-Chn-Mob model. The probabilities are reduced by more than 50% when the mobility models are considered. 3-AP-Chn model yielded 1.9% of unsuccessful handover probability that has missed to happen, where as it is 0.5% in 3-AP-Chn-Mob model when the number of free channels available is just one in the target AP.

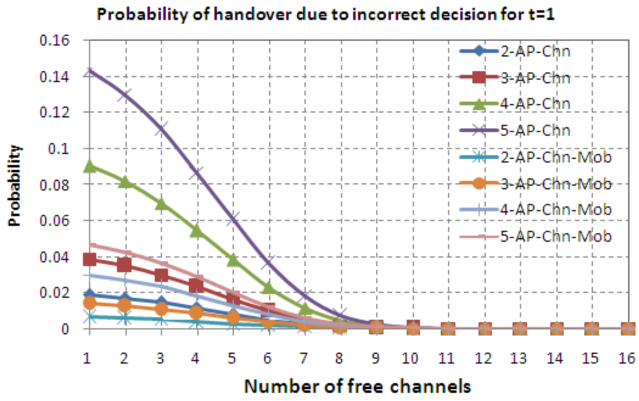


Figure 8 : Total probability of the unsuccessful handoverfor cases with only free channel and free channel plus mobility considered as criteria

Fig. 8 shows the total probability of the unsuccessful handover that has happened for case 1 with only free channel; and free channel plus mobility care considered as criteria, when the mobile node was moving normal to the boundary of the service zone and for the case 1 scenario. The highest probability occurs at 1 free channel with 5-AP-Chn model with 4.5% probability for 5-AP-Chn-Mob model and lowest of 0.9% for 2-AP-Chn-Mob model.

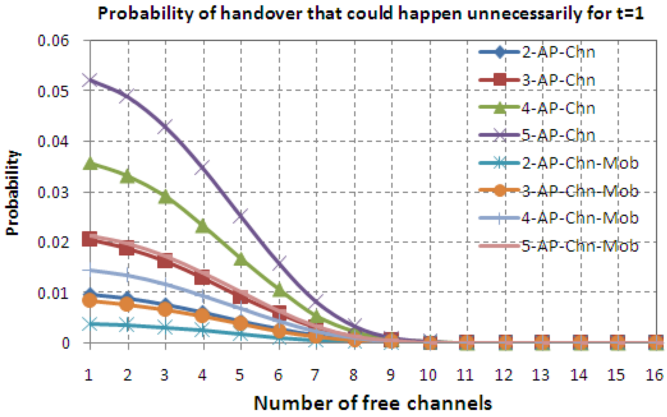


Figure 9 : Probability of the handover that has happened unnecessarily for cases with only free channel and free channel plus mobility considered as criteria

Fig. 9 shows that when there is 1 free channel, the unsuccessful handover probability is 5.2% for the 5-AP-Chn model, and it is 2.1% for 5-AP-Chn-Mob model. The probabilities are reduced again by around 50% when the mobility models are considered. 4-AP-Chn model yielded 3.5% of unsuccessful handover probability that has happened unnecessarily, where as it is 1.5% in 4-AP-Chn-Mob model when the number of free channels available is just one in the target AP. It can be observed that the probabilities have not changed much between the cases of the mobile device moving normal to the boundary to the case of mobile device moving along the boundary, when handover that has happened unnecessarily are considered.

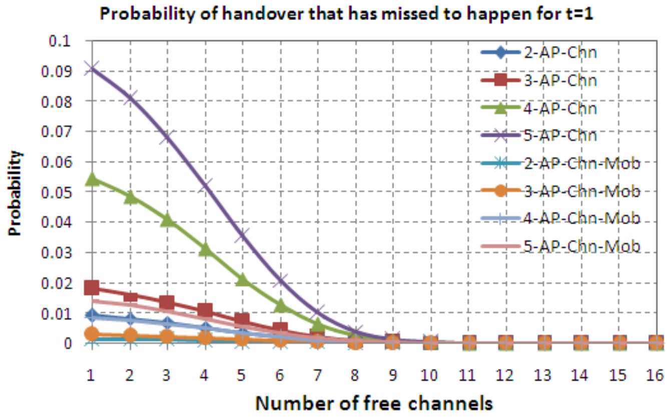


Figure 10 : Probability of the handover that has missed to happen for cases with only free channel and free channel plus mobility considered as criteria

Fig. 9 shows the probability of the handover that has missed to happen. It is clear from Fig.9 that when there is 1 free channel, the unsuccessful handover probability is 1% for the 2-AP-Chn model, and it is 0.2% for 2-AP-Chn-Mob model. The probabilities are reduced by around80% when the mobility models are considered. 3-AP-Chn model yielded 1.9% of unsuccessful handover probability that has missed to happen, where as it is 0.4% in 3-AP-Chn-Mob model when the number of free channels available is just one in the target AP.It can be observed again that the probabilities have not changed much between the cases of the mobile device moving normal to the boundary to the case of mobile device moving along the boundary, when handover that has happened unnecessarily are considered also.

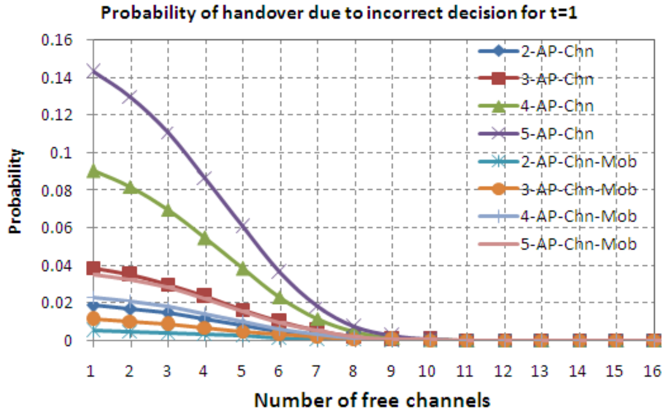


Figure 11: Total probability of the unsuccessful handoverfor cases with only free channel and free channel plus mobility considered as criteria

Fig. 11 shows the total probability of the unsuccessful handover that has happened for case 3 with only free channel; and free channel plus mobility care considered as criteria, when the mobile node was moving along the boundary of the service zone and for the case 3 scenario. The highest probability occurs at 1 free channel with 5-AP-Chn model with 3.5% probability for 5-AP-Chn-Mob model and a lowest of 0.5% for 2-AP-Mob model. It can be observed again that the there is not much improvement in probabilities between the cases of the mobile device moving normal to the boundary to the case of mobile device moving along the boundary, when handover that has happened unnecessarily are considered also. The reason behind this behavior may be attributed to the fact that the historical probability distributions between 8 different turns in Case 1 and Case 2 are almost similar, which is evident from Table 1. However when these distributions are different from each other, a huge difference in the results can be observed.

V. Conclusion

In this work, the handover probabilities for the cases of handover that happened unnecessarily, that has missed to happen and total unsuccessful handover are modeled for the cases of the mobile device moving normal to the boundary and along the boundary of the service zone of AP . Three cases of mobile nodes moving in different set of paths are analyzed and a common procedure is developed to derive the method of computing the handover probabilities. 2-AP, 3-AP, 4-AP and 5-AP models are run by considering only the free bandwidth and free bandwidth plus mobility. The historical data of the probabilities for the movement of mobile devices in pre-identified paths are very important to compute the probability of the mobile device of interest when moving near the boundary. It has been demonstrated that there was more than 50% of improvement in the results when mobility is also considered into the model. Also two cases of historical probability distributions are simulated, and both have yielded similar results since the distribution pattern of historical data is almost same. Probability of the handover that has happened unnecessarily for case 1 and case 3 are 0.4457 and 0.4042 respectively, when only mobility is considered, where as it is 0.2538 and 0.1554 for the probability of the handover that has missed to happen. Since the probabilities between case 1 and case 3 are close to each other for mobility alone, the total probabilities when considered along with free bandwidth is also close to each other.

References References References

1. C. Chi, X. Cai, R. Hao and F. Liu “Modeling and Analysis of Handover Algorithms” IEEE GLOBECOM 2007 proceedings.
2. D. Wong and D.C. Cox. Estimating local mean signal power level in a Rayleigh fading environment. IEEE Trans. Veh. Technol., 48(3):956-959, May 1999.
3. Akhila. S, Suthikshn Kumar, Sambasiva Rao 2012 “Study of multiple parameter algorithm for wrong decisions in vertical handovers in wireless heterogeneous networks”, Elixir Network Engg., ISSN: 2229 – 712X.
4. Akhila. S 1 , V. Sambasiva Rao2, Mobility Algorithm Based on the Prediction of Wrong Decisions for Vertical Handover, International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 5, July - 2012 ISSN: 2278-0181
5. R. Vijayan and J. M. Holtzman. A model for analyzing handoff algorithms. IEEE Trans. Veh. Technol., 42(3):351-356, Aug. 1993.
6. T. Camp, J. Boleng, and V. Davies. A survey of mobility models for ad hoc network research. Wireless Commun. & Mobile Computing, 2(5):483-502, Sep. 2002. Special issue on Mobile Ad Hoc Networking: Research, Trends and Applications.
7. Ch.Subrahmanyam and K.Chennakesava Reddy. Generalized Probability Model in a WPAN to Compute Handover Probabilities, International Journal of Computer Applications(IJCA) Vol.126 5,October 2015.
8. T. M. Ali, M. Saquib, and C. Sengupta. Vertical handover analysis for voice over WLAN/cellular network. In Proc. IEEE Int. Conf. on Commun., May 2010.

9. A. H. Zahran and B. Liang. Performance evaluation framework for vertical handoff algorithms in heterogeneous networks. In Proc. IEEE Int. Conf. on Commun., 2005.
10. J. Broch, D. A. Maltz, D. B. Johnson, Y. C. Hu, and J. Jetcheva. A performance comparison of multi-hop wireless ad hoc network routing protocols. In Proc. Int. Conf. on Mobile Computing and Networking, 1998.
11. T. M. Ali, M. Saquib, and C. Sengupta. Performance analysis framework and vertical handover triggering algorithms for voice over WLAN/cellular network. In Proc. IEEE Wireless Commun. and Networking Conf., Apr. 2008.
12. R. Prakash and V. V. Veeravalli. Adaptive hard handoff algorithms. IEEE J. Select. Areas Commun., 18(11):2456-2464, Nov. 2000.

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 15 Issue 7 Version 1.0 Year 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Identity Mapping Scheme with CBDS Approach to Secure MANET

By Gaurav Jain, Rajdeep Shaktawat & Kalpana Jain

College of Technology and Engineering, India

Abstract- A MANET is considered as self administrating network in which nodes are free to come and join to communicate with various nodes. A network which has a lot of advantages for its characteristics also has disadvantage of being attacked by some malicious node. Since MANET requires that each node should posses a unique, distinct identity, Sybil attack is one of the major threat to MANET. A Sybil attack is in which a node can have different physical identity to weak the distributed MANET system. In this paper, we propose a identity mapping scheme which is implemented with the collaborative bait detection scheme for securing MANET against Sybil attack, black hole attack and gray hole attack. Approach is merged with the CBDS approach for making system more secure against various attacks. Proposed scheme is simulated on NS2 and compared with the Sybil detection scheme on various performance metrics.

Keywords: manet, secure network, identity mapping scheme, sybil attack, black hole attack, gray hole attack.

GJCST-E Classification : *D.2.1*

IDENTITYMAPPINGSCHEMEWITHCBDSAPPROACHTOSECUREMANET

Strictly as per the compliance and regulations of:

Identity Mapping Scheme with CBDS Approach to Secure MANET

Gaurav Jain [α], Rajdeep Shaktawat [σ] & Kalpana Jain [ρ]

Abstract- A MANET is considered as self administrating network in which nodes are free to come and join to communicate with various nodes. A network which has a lot of advantages for its characteristics also has disadvantage of being attacked by some malicious node. Since MANET requires that each node should posses a unique, distinct identity, Sybil attack is one of the major threat to MANET. A Sybil attack is in which a node can have different physical identity to weak the distributed MANET system. In this paper, we propose a identity mapping scheme which is implemented with the collaborative bait detection scheme for securing MANET against Sybil attack, black hole attack and gray hole attack. Approach is merged with the CBDS approach for making system more secure against various attacks. Proposed scheme is simulated on NS2 and compared with the Sybil detection scheme on various performance metrics.

Keywords: manet, secure network, identity mapping scheme, sybil attack, black hole attack, gray hole attack.

I. Introduction

The MANET (Mobile Ad hoc Network) are widely used in various applications like military application and in emergency operations due to mobility of nodes in wireless network. Every node depends on one another so coordination between them become important, if any of the node misbehave or do not coordinate, it can lead to destruction of whole MANET. One such attack is Sybil Attack in which a node can posses multiple identity. In such type of attack a node posses some other node identity and thus participate itself on behalf of genuine node, thus harming the integrity and security among nodes.

A network in which any node can join and leaves the network without any central authentication, breaching such a network is simple for any malicious node. So the security comes out to be the important aspect in MANET. In MANET each node should have only a single identity through which it can communicate with other nodes in the network. In MANET each node act as a host as well as router, this significant feature of MANET also comes with the serious drawback of security issue. As path between the source and destination has number of nodes in between which act as router and transfer data from one end to another. The nodes are free to move so there is no fix topology in this network, this gives a fair chance to any malicious node to come and break the integrity of the network.

In this approach, there is collaborative bait detection scheme which is merged with the ID mapping scheme to secure the MANET against various black hole attack, gray hole attack and Sybil attack.

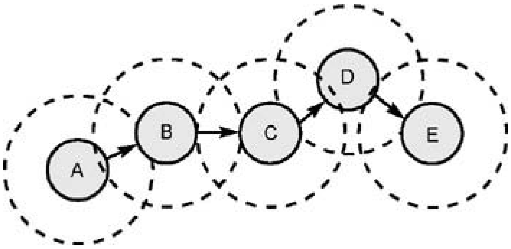


Fig.1: A Simple MANET structure

A node can transfer or communicate with the node which falls in their radio range. Before the data transmission takes place between the source and destination, source needs to find out the location of the destination as in MANET nodes are free to join or leave the network or move freely. There is no central authority which governs the whole network or the communication so it totally depends upon the nodes to find the destination node and its path. Intermediate nodes work during the path formation as well as during the data transmission. Broadly there are two categories of routing protocols in MANET, one in which path formation or routing takes place when source needs to communicate with the destination and second in which all nodes exchange some packets continuously to keep the path for each node. As there is power constraint in MANET on demand routing protocols are much preferred than table driven protocols.

MANET network is much exposed to various threats due to its characteristics. There are various attacks for which MANET is exposed, held at different layers. Many attacks are performed during routing like a malicious node can change various fields of route discovery packet which can result in a path formation in which malicious node fall, after that a malicious node can perform various attacks like black hole and gray hole attack which result in rapid degradation of network as malicious node starts dropping of data packet for all connection in black hole attack and for a particular connection in gray hole attack. The other major attack is Sybil attack in which attacker can disrupt location-based or multipath routing by participating in the routing.

Author α σ ρ: Computer Science and Engineering, College of Technology and Engineering, India. e-mails: shaktawat.rd@gmail.com, gauravpamecha20@gmail.com, kalpana_jain2@rediffmail.com

a) Characteristics of MANET

Dynamic Topology : In MANET the nodes are free to move with different speed , due to which the topology changes frequently.

Security: MANET is an open network no authentication of nodes. So they are more prone to attacks like black hole, grayhole , Sybil and other attacks.
Multi hop routing: When a node tries to send information to other nodes which is out of its scope, the packet forwarded via one or more intermediate nodes.

Distributed operation: There is no central control or authority in MANET which controls the movement of nodes in MANET. The nodes collaborate and broadcast among themselves.

b) Challenges in MANET and Security

Limited bandwith : The narrow radio band results in decreased data rates compared to the wireless networks. Hence minimum use of bandwidth is necessary by keeping low overhead as possible.

Routing Overhead: In MANET, nodes often change their location within network, which leads to unnecessary routing overhead.

Packet Loss : There is higher packet loss because of increased collisions by the presence of hidden terminals, presence of interference, unidirectional links, frequent path breaks due to mobility of nodes.
Hidden terminal problem: The hidden terminal problem refers to the strike of packets at a accepting node due to the simultaneous transmission of those nodes that are not within the direct communication range of the sender, although are in the transmission range of the receiver

Security threats: As the MANET is liable to eavesdropping and wireless system functionality is established through node cooperation, mobile ad hoc networks are exposed to numerous security attack like blackhole, grayhole ,Sybil attacks etc.

II. Background details

There are two approach for security in all network one is Preventive approach that is cryptographic approach in which different cryptography processes are used for guard and second is reactive approach in which systems like intrusion detection systems are used for tracking down attacks like IP spoofing, blackhole, grayhole, Sybil attack etc. This paper will concentrate in one protocol DSR standardized by IETF. The fundamental difference that is in between DSR networks and established internet protocol is the security. That draws attention of many researchers over this note. DSR networks are more prone to any attacks. Attacks in DSR network is not only constitute of modification, eavesdropping, Sybil attacks etc. but also like nodes not cooperating in routing, intentionally dropping the packets, changing contents that attract source and destination to choose This paper will discuss approaches that are used so far for security and the proposed scheme proves out to be more capable in terms of security with minimum overhead and maximum security. This paper proposed a detection scheme called the cooperative bait detection scheme (CBDS) with ID mapping scheme, which aims at identifying and hampering malicious nodes launching grayhole, blackhole along with Sybil attack in MANET.

a) Coolabrative Bait Detection Scheme (CBDS) Approach

The cooperative bait detection scheme (CBDS), which plan at detecting and preventing malicious nodes launching grayhole/collaborative blackhole attacks in MANETs. In this approach, the source node stochastically selects an adjacent node with which to collaborate, such that the address of this node is used as bait destination address to bait malicious nodes to send a route reply RREP information. Malicious nodes are then detected and prevented from participating in the routing procedure, applying a reverse tracing technique. In this scheme, it is assumed that when a significant drop occurs in the packet transmission ratio, an alarm is emit by the destination node back to the source node to trigger the detection mechanism again.
CBDS scheme merges the advantage of proactive detection in the initial step and the superiority of reactive feedback at the successive steps in order to lower the resource wastage. CBDS is DSR-based. As such, it can identify all the addresses of nodes in the elected routing way from a source to destination after the source has accepted the RREP message. However, the source node can not necessary capable to identify which of the intermediate nodes has the routing knowledge to the destination or who has the reply RREP message or the malicious node reply forged RREP.

This scenario can result in including the source node sending its packets through the fake shortest path chosen by the malicious knot, can result to a blackhole attack. To resolve this issue, the function of HELLO message isjoined to the CBDS to assist each node in identifying which nodes are their adjacent nodes within one hop. This function helps in sending the bait address to seduce the malicious nodes and to utilize the reverse tracing program of the CBDS to identify the perfect location of malicious nodes. The baiting RREQ packets are similar to the original RREQ packets, but their target address is the bait address.

i. Initial Bait Setup

The aim of the bait phase is to seduce a malicious node to send a reply RREP by sending the bait RREQ which it has used to announce itself of containing the shortest path to the node that detains the packets that were converted. To accomplish this goal, the subsequent method is created to generate the destination address of the bait RREQ’. The source node randomly pick an adjacent node, i.e., *nr*, within its one-hop neighborhood nodes and cooperates with this node by catching its address as the destination location of the bait RREQ'. Since each baiting is done stochastically and the adjacent node could be altered if the node moved, the bait would not remain same. The bait phase is activated whenever the bait RREQ' is sent earlier to seek the first routing path.

ii. *Reverse Tracing Setup*

The reverse tracing approach is used to discover the nature of mischievous nodes through the route reply to the RREQ' message. If a mischievous node has taken the RREQ, it will reply with a fake RREP. Accordingly, the reverse tracing action will be applied for nodes receiving the RREP, with the aim to find out the malicious path information and the momentary trusted region in the route. It should be emphasized that the CBDS is capable of detecting more than one malicious node parallel meanwhile these nodes send reply RREPs. Indeed, when a malicious node, for example, *nm*, answer with a fake RREP, an address table P = {n1, . nk, . . . nm, . . . nr} is stored in the RREP. If node *nk* receive the RREP, it will isolate the *P* list through the destination address *n*1 of the RREP in the IP field and get the address list Kk = {n1, . . . nk}, where *Kk* show the route knowledge from root node *n*1 to destination node *nk*. Then, node *nk* will identify the diversity between the address list P = {n1, . nk, . . . nm, . . . nr} stored in the RREP and Kk = {n1, . . . nk}

b) *RSS Sybil detection Approach*

In particular, this scheme utilizes the Received Signal Strength (RSS) value in order to identify among the legitimate and Sybil knot. It presume that the attacker conjoin the network with its one identity, and that malicious nodes do not conspire with one another. It also infer that nodes do not rise or drop their transmit power.

The difference between a new legal node and a new Sybil identity can be made found on their neighbourhood joining nature.

The new authentic nodes become neighbours when they arrive inside the radio range of another nodes; thus their first RSS at the receiver node will be low .

On contradiction a Sybil attacker, which is already a neighbour, will result its new identity to appear suddenly in the neighbourhood.

Each node keep a list of neighbours in the form

<Address, Rss-List <time, rss>>.

Every node will catch and stock the signal strength of the transmissions received from its neighbouring nodes.

It Does not detect Sybil node present in root

III. The Proposed Method

a) *ID Mapping Scheme for Sybil Attack*

In the CBDS approach, the reverse tracing technique is used to find the blackhole and grayhole attack in MANET. The address list has been attached with the RREP, by splitting out and finds the intersection of that address list only we find out temporary trusted identities and the malicious list. So, identity of a node is very much important in the reverser tracing technique.

But in Sybil attack, more than one identity can correspond to a single entity. To detect the Sybil identity present in the network, we are going to mapping the id with the entity or node in the network. For that, we propose a new scheme called **as ID mapping scheme.**

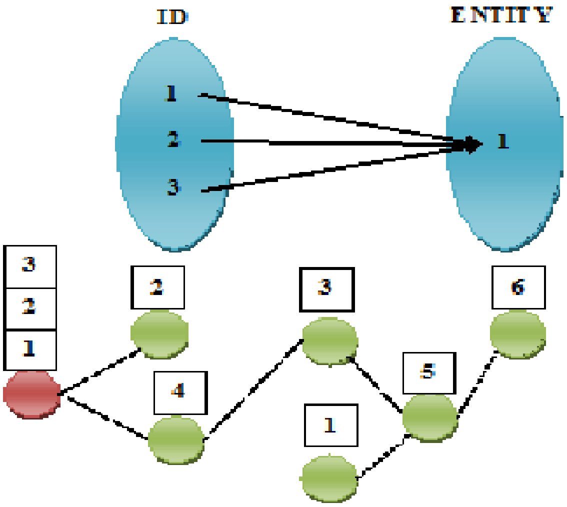
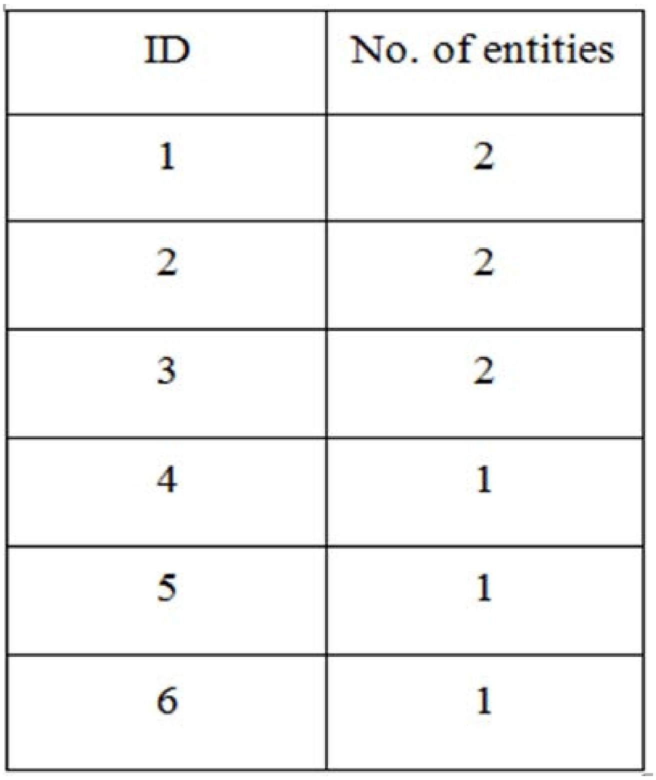


Fig 2 : Id Mapping

After detecting the temporary trusted list the source node the source node check for Sybil identity in the network. The Sybil node is having more than one identity to act as multiple nodes in the network simultaneously. The source node runs the following algorithm to detect the Sybil identities in the network. Before that, the source node maintains a table in the following format

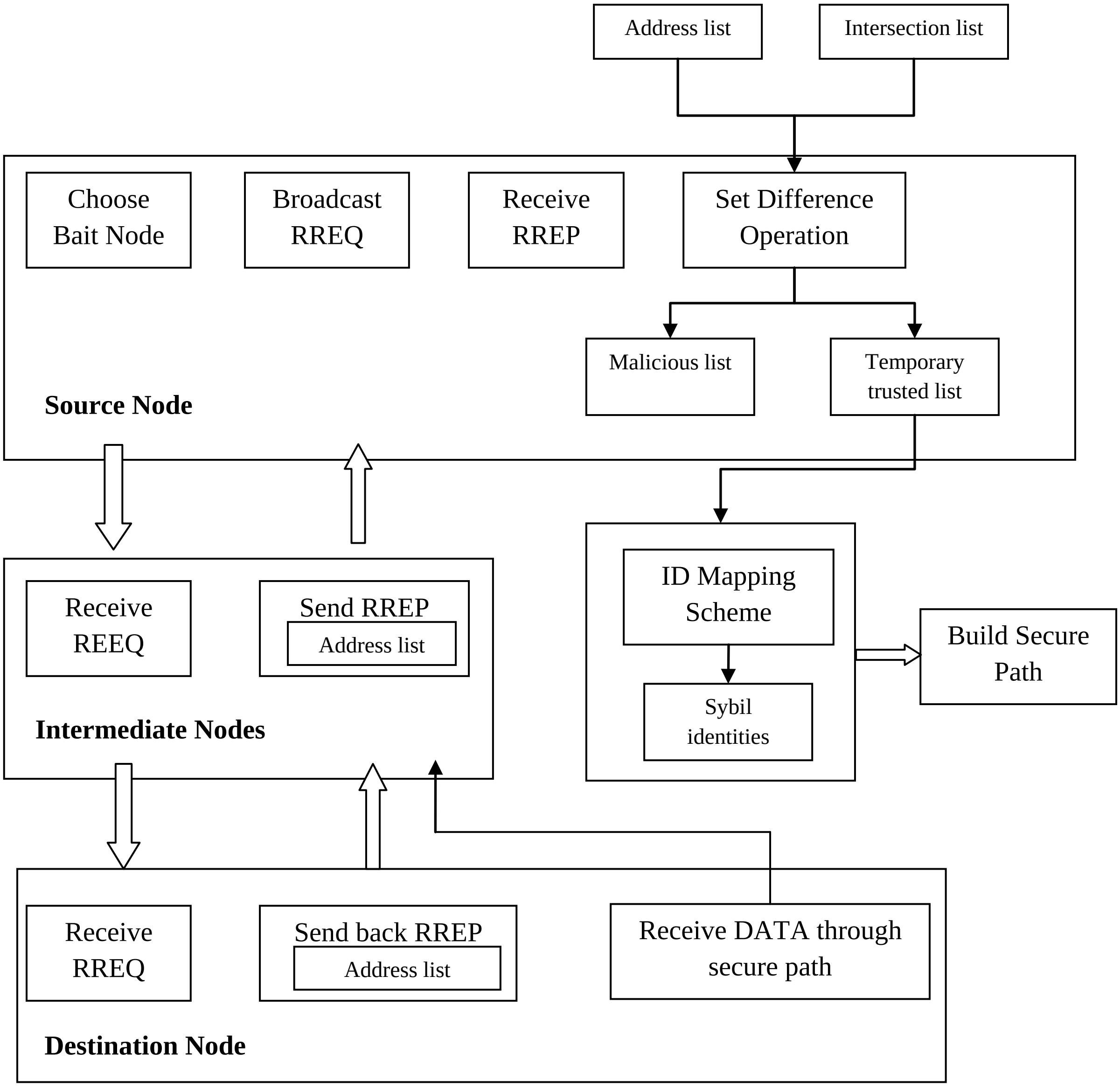


ID	No. of entities
1	2
2	2
3	2
4	1
5	1
6	1

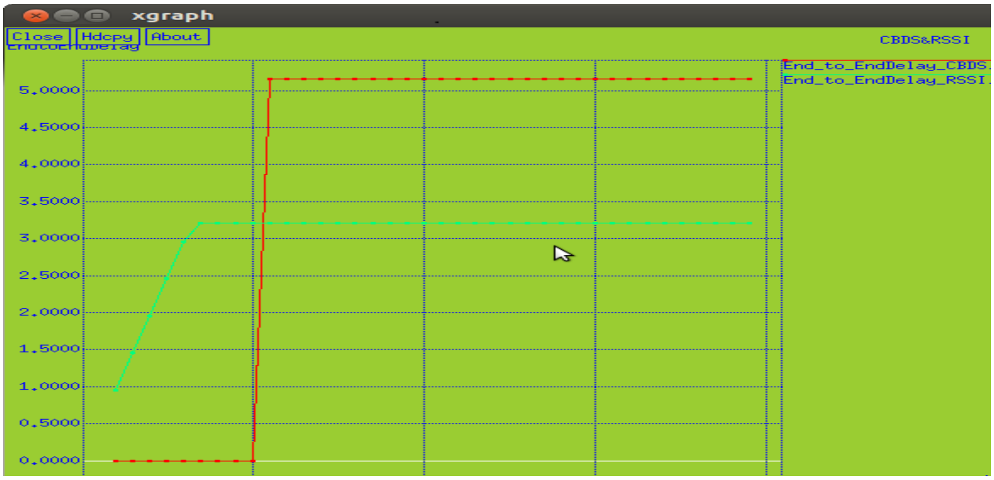
ID mapping scheme:

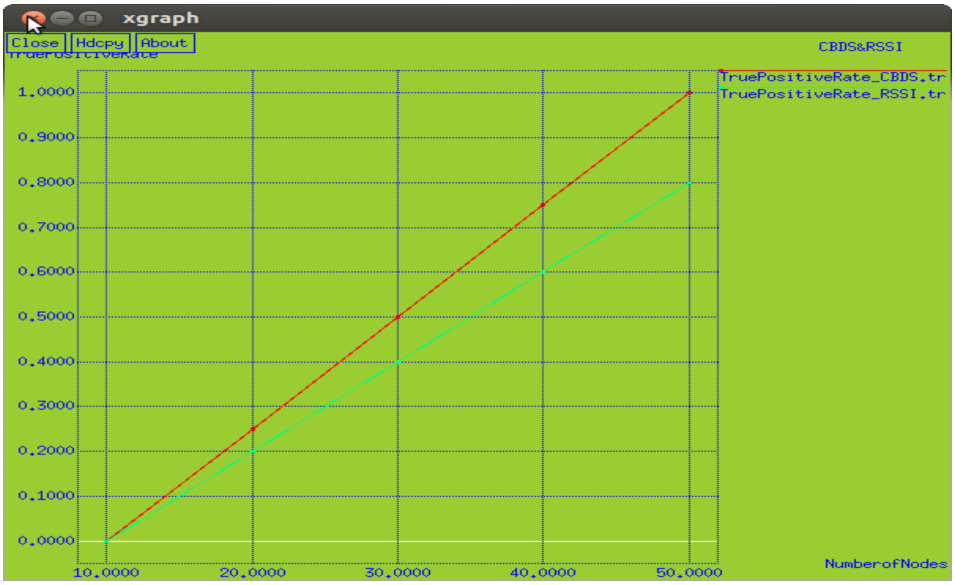
```
For each node ‘n’ in trusted list
{
        Nid=n
        While (Not reach all the nodes) {
                Source node broad cast hello message
                If (source receives reply with source address n) {
                        Increment no. of entities by 1
                }
        }
        If(no. of entities>1) {
                Insert node with id ‘n’ to the malicious list
        }
}
```

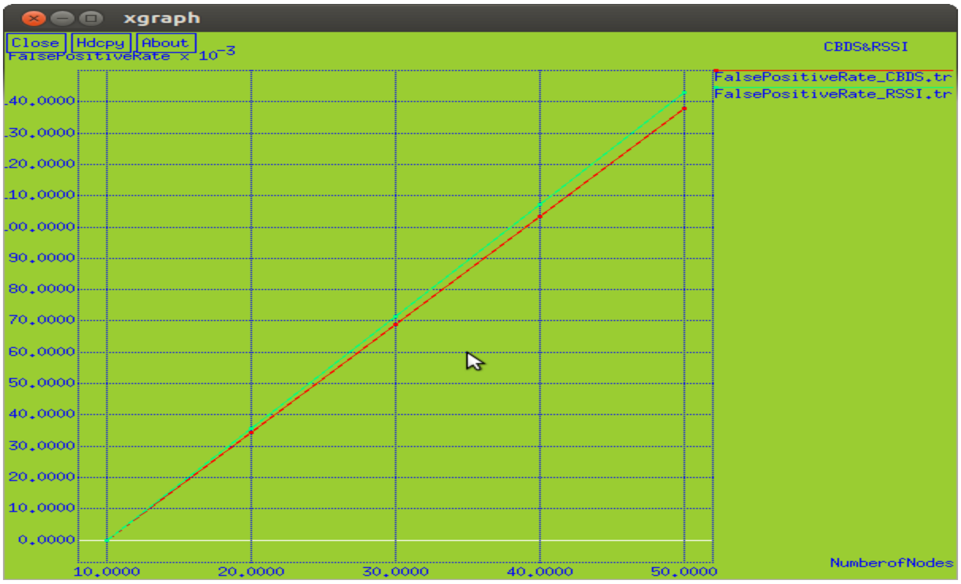
Block Diagram

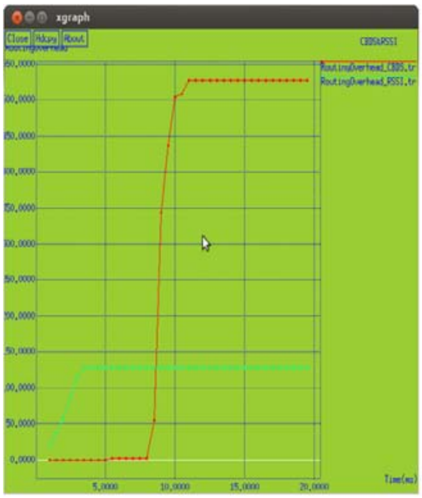


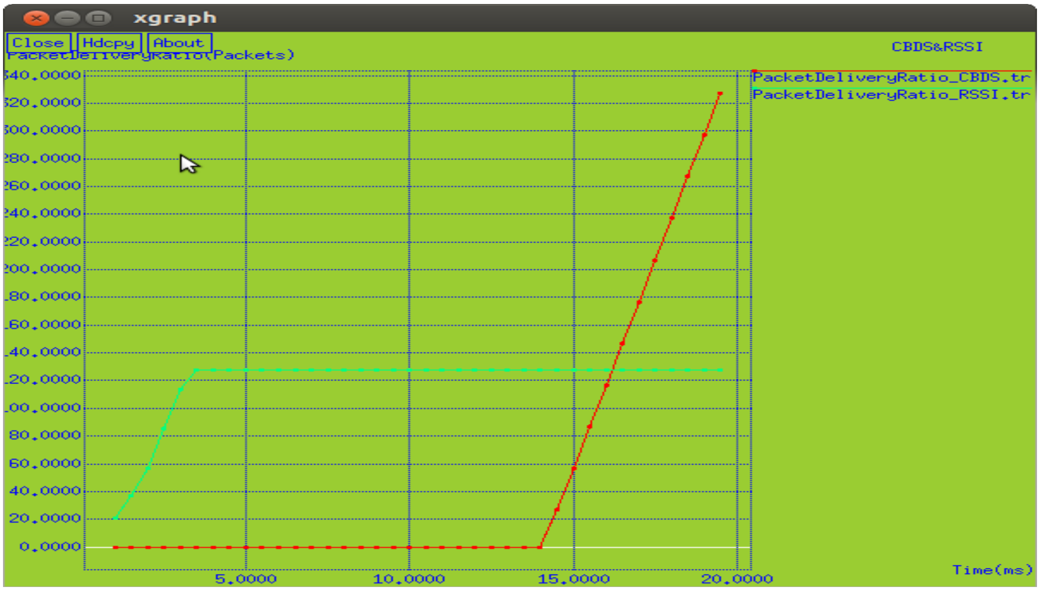
IV. Implementation and Results




xgraph
Close
Hdcpy
About
TruePositiveRate
CBDS&RSSI
TruePositiveRate_CBDS.tr
TruePositiveRate_RSSI.tr
1.0000
0.9000
0.8000
0.7000
0.6000
0.5000
0.4000
0.3000
0.2000
0.1000
0.0000
10.0000
20.0000
30.0000
40.0000
50.0000
NumberofNodes


xgraph
Close
Hdcpy
About
FalsePositiveRate x 10^{-3}
CBDS&RSSI
FalsePositiveRate_CBDS.tr
FalsePositiveRate_RSSI.tr
40.0000
30.0000
20.0000
10.0000
00.0000
90.0000
80.0000
70.0000
60.0000
50.0000
40.0000
30.0000
20.0000
10.0000
0.0000
10.0000
20.0000
30.0000
40.0000
50.0000
NumberofNodes


xgraph
Close
Hdcpy
About
RoutingOverhead
CBDS&RSSI
RoutingOverhead_CBDS.tr
RoutingOverhead_RSSI.tr
50,0000
00,0000
50,0000
00,0000
50,0000
00,0000
50,0000
00,0000
50,0000
00,0000
50,0000
0,0000
5,0000
10,0000
15,0000
20,0000
Time(ms)



V. Conclusion and Future Work

This paper attempts to resolve the problem of presence of malicious node which leads to black hole/ gray hole and Sybil attack in MANET which is referred to as the cooperative bait detection scheme (CBDS) with ID Mapping Scheme, that integrates the advantages of both proactive and reactive defense architectures. Our CBDS method implements a reverse tracing technique to help in achieving the stated goal. In this project, we have proposed a new mechanism (called the CBDS) for detecting malicious nodes in MANET's under gray/collaborative blackhole attacks. The ID Mapping scheme is used to detect the Sybil node present in the network. Our simulation results revealed that the CBDS with ID mapping scheme outperforms than the existing method RSSI based Sybil detection scheme in terms of routing overhead, End to End delay and packet delivery ratio.

References References Referencias

1. Baadache and A. Belmehdi, "Avoiding blackhole and cooperative blackhole attacks in wireless ad hoc networks," *Intl. J. Comput. Sci. Inf. Security*, vol. 7, no. 1, 2010.
2. K. Liu, D. Pramod, K. Varshney, and K. Balakrishnan, "An Acknowledgement based approach for the detection of routing misbehavior in MANETs," *IEEE Trans. MobileComput.*, vol. 6, no. 5, pp. 536–550, May 2007.
3. S. Abbas, M. Merabti, D. Llewellyn-Jones, and K. Kifayat, "Lightweight Sybil Attack Detection in MANETs", IEEE Trans., vol. 7, no. 2, June 2013.
4. W. Wang, B. Bhargava, and M. Linderman, "Defending against collaborative packet drop attacks on MANETs," in *Proc. 28th IEEE Int. Symp. Reliable Distrib. Syst.*, New Delhi, India, Sep. 2009.
5. I. Chlamtac, M. Conti, and J. J.-N. Liu, "Mobile ad hoc networking: Imperatives and challenges," *Ad Hoc Netw.*, vol. 1, no. 1, pp. 13–64, 2003.
6. J. R. Douceur, "The Sybil attack," presented at the Revised Papers from the First Int. Workshop on Peer-to-Peer Systems, 2002, pp. 251–260.
7. J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: Analysis and defences," presented at the 3rd Int. Symp. Information Processing in Sensor Networks (IPSN), 2004, pp. 259–268.
8. B. Parno and A. Perrig, "Challenges in securing vehicular networks," in *Proc. 4th Workshop HotNets*, 2005, pp. 1–6.
9. K. Hoeper and G. Gong, "Bootstrapping security in mobile ad hoc networks using identity-based schemes," in *Security in Distributed and Networking Systems* (Computer and Network Security). Singapore: World Scientific, 2007.
10. S. Hashmi and J. Brooke, "Toward Sybil resistant authentication in mobile ad hoc networks," in *Proc. 4th Int. Conf. Emerging Security Inform., Syst. Technol.*, 2010, pp. 17–24.

This page is intentionally left blank

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 15 Issue 7 Version 1.0 Year 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Metrics for Quality Assurance of Web based Applications

By Qasim Zia
FAST-NU University, Pakistan

Abstract- Web-Commerce applications are now an indispensable aspect of businesses around the world. More businesses are now migrating from outdated applications to a new type of combined e-business designs. With such large volumes of applications that need to be put online, there is now a dire need for measurable and quantifiable metrics that can help in gauging the quality of these websites.

The development considerations for both domains may be deemed similar in their final purpose, that is to provide a service to its end-users, however, web-applications today face a myriad of constraints, with most businesses opting to go online, the crucial questions are; Is the Web info metrics are any different, or is it just an application of classical metrics (desktop metrics) to a new medium (web metrics).

In our research, we propose to investigate these issues, and present the distinguishable metrics for the Quality Assurance(QA) processes involved in Web-Applications, as opposed to traditional desktop software application.

Keywords: metrics; measurements; websites; web applications; vulnerabilities; requirements; testing.

GJCST-E Classification : H.3.5

Metrics for Quality Assurance of Web based Applications

Qasim Zia

Abstract- Web-Commerce applications are now an indispensable aspect of businesses around the world. More businesses are now migrating from outdated applications to a new type of combined e-business designs. With such large volumes of applications that need to be put online, there is now a dire need for measurable and quantifiable metrics that can help in gauging the quality of these websites.

The development considerations for both domains may be deemed similar in their final purpose, that is to provide a service to its end-users, however, web-applications today face a myriad of constraints, with most businesses opting to go online, the crucial questions are; Is the Web info metrics are any different, or is it just an application of classical metrics (desktop metrics) to a new medium (web metrics).

In our research, we propose to investigate these issues, and present the distinguishable metrics for the Quality Assurance(QA) processes involved in Web-Applications, as opposed to traditional desktop software application. We will also be scrutinizing the major problem that has been persistent in QA related to web applications; the lack of standards, and development models for the web applications.

Keywords: metrics; measurements; websites; web applications; vulnerabilities; requirements; testing.

I. Introduction

Businesses around the world are now migrating from outdated desktop applications to a new class of combined e-business architectures. As the time progresses, businesses will continue to adopt e-business more and more. Metrics are the basic assets of any organization because they deliver appropriate data and information which is used for examining, directing, observing and endorsing [1]. Metrics and Measures values should be replica table and match able between the projects of organization in order to make the examination and policy making processes more strong. With such large volumes of applications that need to be put online, there is now a dire need and motivation for measurable and quantifiable metrics that can help in evaluating the quality of these websites.

The key areas for a web-commerce application that we identified in terms of relevance to the business, the technologies used locally in Pakistan as well as the interests of the stakeholders in Web Projects can be summed up as:

i. *Performance*

In E-Commerce applications, performance issues can be critical since the time to perform any business case or function dictates the actual capability of the system.

ii. *Security*

Online security is perhaps overlooked most often in local software-houses; websites with poor security implementations will invariably damage users and the business.

iii. *Ease of Use*

Quality issues regarding the ease of use of a web application are important in sense that they help a business to retain their client age. Also, such applications are easier to maintain and change.

iv. *SE Optimization or Page Strength*

Search Engine optimization is an important quality aspect in the context of an e-commerce application. Page visibility and rankings can be very important in the web-commerce industry.

v. *Portability*

With a growing range of computer hardware and software platforms, it is important for ecommerce applications to be able to perform consistently and provide similar functionality in different computing environments.

vi. *Reliability*

As with traditional desktop software development and online web application development, reliability is always an important quality issue for users[3]. A web application should always produce consistent results and outputs for a given fixed input. Otherwise the application cannot be trusted for high quality service.

A classical approach to Quality Assurance for online applications would be to gather metrics data from a pre-defined set of metrics. The main problem is that the traditional desktop metrics that have been identified for conventional or non-web related applications could understandably fall short of the mark when applied to the domain of web technologies even though if the development considerations for both domains may be deemed similar in their final purpose that is to provide a service to its end-users.[4] This is because of the fact that websites are being accessed by billions of users

Author: Department of Computer Science and Information Technology, FAST-NU University, Lahore 54000, Pakistan. Tel: +923234400172 e-mail: qasim_233@yahoo.com

and every user has its own opinion about the quality of website.

In this paper, we wish to investigate whether the traditional desktop metrics approach is as useful in this domain or not. We will also be scrutinizing the applicability of metrics data to online applications quality assurance and judge whether Website QA is any different from traditional desktop software Quality assurance practices.

We wish to analyse the quality assurance issues related with website development, for this we will be focusing on the key aspects of a website application. The domain of these integrated web-applications will be e-commerce sites. Keeping above quality aspects in mind we propose to move forward with an analysis based upon some of the e-commerce releases and projects from the local market.

So, a variety of research queries was designed distributed by issues as discussed above[5]:

- What are the common metrics requirements for web applications and desktop software applications?
- What are the vulnerabilities found in performance testing?
- What are the impacts on results?

II. Research Methodology

For our research, we will be using real world project from the local software producers in Pakistan. Our main aim is to first identify a set of key quality aspects and then formulate a workable model for the proper validation of the quality metrics thus identified[6]. To address the problem we have developed a model for this study (shown in figure 1).

A breakdown of the model can be represented as follows:

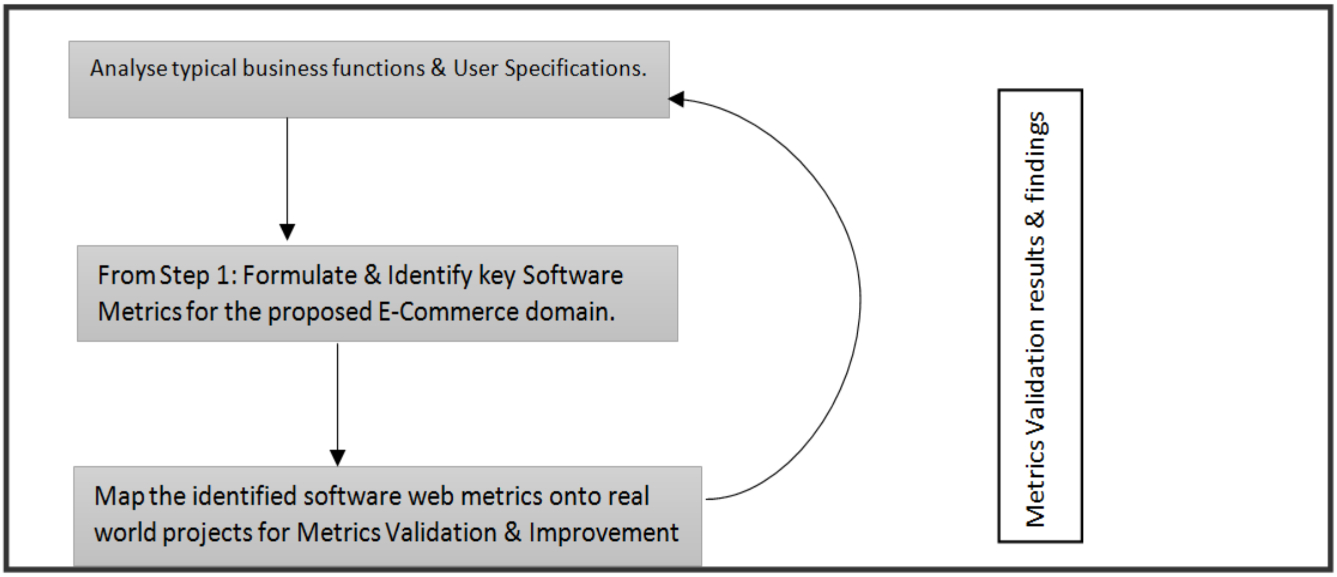

Analyse typical business functions & User Specifications.
From Step 1: Formulate & Identify key Software Metrics for the proposed E-Commerce domain.
Map the identified software web metrics onto real world projects for Metrics Validation & Improvement
Metrics Validation results & findings

Figure 1 : Conceptual Model for Metrics Identification & Improvement

The above model can assist us in obtaining a fairly consistent set of Web-Metrics that are actually derived from the Client Specifications, keeping the most critical and demanded business functions in view.

III. Research Site and Data Collection

To support our research on the identification of web-metrics for online applications, we selected the most readily available test data and plans used for an Urdu localization project: An Online Urdu Dictionary (OUD) [7]. The main emphasis of these tests was to test the application for stress conditions and system robustness. The data collected consists mainly of performance testing done on the system, involving input word parameters to the system and gauging the response time of the system.

The tests also involved system search performances by using different word lengths. A detail of the parameters involved in these tests is shown in Table 1 & Table 2.

Table 1: Data Parameters used for Performance Testing

<Function ID>	Response Times
Exact Word	
Using Wild Cards	
Idioms	
Idioms with wildcard	
Input Parameters(Actual Words)	

Table 2 : Search Test parameters and Result Criteria

Wrong Word	Intended Word	Total Results	Start Time	End Time	Total Time

The OUD concentrated their efforts on Performance and Reliability Testing. The Performance was tested on a different set of browser platform, however quality issues such as portability, ease of use were not looked into[8]. For our sample project, the criticality of security and search engine optimization was relatively low.

IV. Research Results and Data Analysis

Detailed results obtained from the above tests were made available to us for further inspection, a snapshot of the results is shown in Figure 1 and Figure 2.

Table 3 : Performance Testing Results

			T1	T2	T3	Average	Worst
Initialize		Response Time (MS)	145.3	143.7	146.8	145.3	146.8
Search Words With Diacritics	Exact	Parameters	پان	آن	ہلور		
		Results	14	5	0		
		Response Time (MS)	32	15	15	20.7	32
	Wildcard	Parameters	ا*	*ات*	*ا*ت*		
		Results	5576	3038	8549		
		Response Time (MS)	391	234	937	520.7	937
	Idioms	Parameters	آب اُڑنا	آگ میں جلانا	اَخْبار نکالنا		
		Results	0	1	1		
		Response Time (MS)	31	125	63	62.5	125
	Idioms With Wildcard	Parameters	آ* اُڑنا	آ؟ میں جلانا	آ* نکالنا		
		Results	6	1	3		

Table 4 : Search Performance Test Results

Wrong Word	Intended Word	Total Results	Position in Results	Position (Percentage)	Start Time (Seconds)	End Time (Seconds)	Duration (Seconds)
2 letter words							
اج	آج	116	2	1.72	19.27	23.48	4.22
مش	ماش	141	26	18.44	30.37	35.64	5.27
چی	جی	177	33	18.64	44.23	49.97	5.74
حن	جن	142	58	40.85	52.09	55.72	3.62
فج	فجر	73	17	23.29	57.98	59.17	1.19
Maximum		177	58	40.85	40.79	44.80	5.74
Average		129.80	27.20	20.59			4.01
3 letter words							
ترد	تردد	90	14	15.56	64.50	67.05	2.55
زکر	ذکر	41	14	34.15	71.87	72.72	0.84
ہمد	حمد	35	5	14.29	77.16	78.25	1.09
ہیپ	ہیپ	44	Not Found	NA	82.70	83.92	1.22
شیب	سیب	75	25	33.33	88.58	91.34	2.77
Maximum		90	25	34.15			2.77
Average		60.25	14.50	24.33			1.81

Total Searches	195
Approximate Searches	30
Percentage Approximate Search	15.38461538
Maximum Result in Approximate Search	124
Average Results per Approximate Search	15.1
Maximum Response Time	6.421
Average Response Time	0.880633333

Table 5 : Statistics Obtained from Search Performance Testing

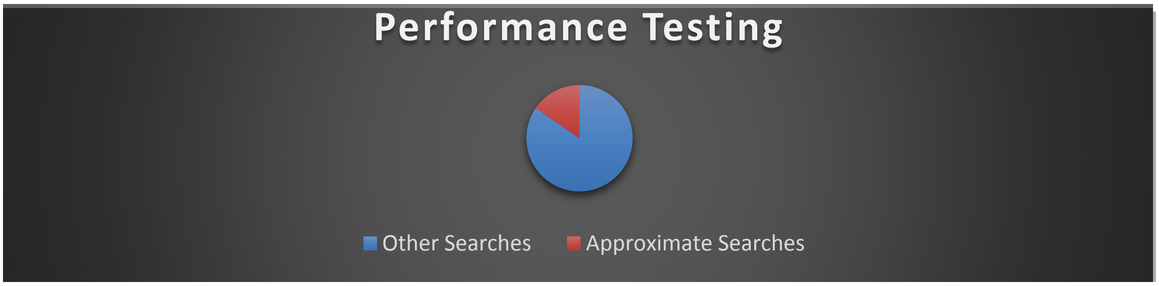


Figure 1.2 : Pie Chart of Performance Testing

V. Discussion of Results Regarding Site

The 'metrics' regarding web metrics states to the size or measuring the quality of websites. Specially, measuring website actions, and take out their trends [9]. Metrics quantify different attributes in terms of software quality, and are helpful to predict software quality quantitatively during development and after the product is in operation, and are considered as the final component of the SQA program [10].

A graphical representation of the E-Commerce Application metrics attributes thus identified is given below [11] (Figure 1.3).

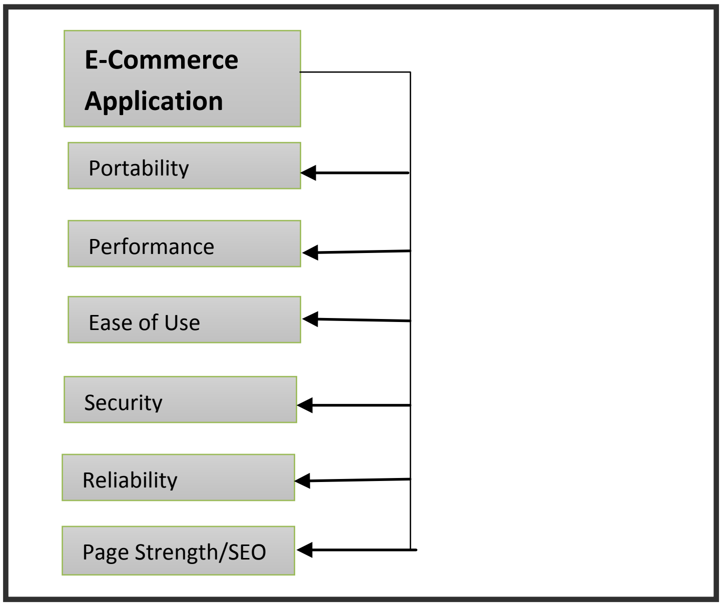


Figure 1.3 : Some of E-Commerce Application Metrics Attributes

The decomposition is based on the quality attributes, and their importance during different phases of product life [12]. Product operation includes development and deployment as well. During the operations Portability, Search Engine Optimization (SEO), Reliability, Usability, Scalability, Security, and Availability are the key attributes identified [13].

For our purposes, we focused on the performance issues related with the Online Urdu Dictionary (OUD). The testing performed on the system was aimed mainly on stress and robustness (Reliability). The results of the tests reveal that:

- For increasing number of word length, the response time also increases linearly.
- Performance of the OUD degrades when input parameters are complex (i.e. the use of wildcards and idioms)
- The average number of results obtained for each search is 15, which is high for most correct searches.
- A maximum response time of 6 seconds is achieved which is very high for all circumstances

VI. Conclusions, Recommendations and Future Work

The aim of our study was to investigate the possible deviations from a traditional desktop software metrics approach applied to online applications. During our study, we identified some key metrics that would be essential to the quality of an Online Application. From our discussions we have gathered that a metrical approach that is followed by desktop applications, is also applicable to an Online Web Domain in some scenarios [14], the underlying issues for our case-study sample, the online Urdu Dictionary were somewhat similar to those encountered for offline applications.

Some of the metrics attributes identified by us in our research methodology leads to better online applications in terms of security, performance, reliability and ease of use. However, the traditional desktop software application metrics are not adequate and relevant to handle the additional specific metrics of web based applications like search engine optimization (SEO) etc. In case of online applications, performance plays an important role as a key metric and adds to more criticality of the online application because business organizations deal with daily transactions and can't afford the risk regarding performance issues.

The Tests regarding the following metrics attributes must be taken on the above mentioned OUD project, in order to cater the quality assurance measures and issues:

- Security
- Ease Of Use
- Search Engine Optimization(SEO) or Page Strength
- Portability

The analysis by the OUD team does not include anything other than performance measure. All the tests include issues like stress testing or result's response time and overall system testing; No doubt it is an essential part of the analysis (performance) but the above mentioned metrics can't be ignored as far as the quality assurance is concerned.

Concerning about future work, results for the other metrics attributes like Portability, Ease of Use, Search Engine Optimization (SEO) and Security/Risk should also be calculated. How much these attributes are beneficial in web based applications as compared to traditional desktop based software applications (attributes which are applicable on non-web desktop based applications). So we are seeing this as its future development. This can help the initialization of more strong policies, procedures, and approaches.

Appendix

Sample Bug Reports Generated For Oud

Test Case ID	Bug ID	Execution Date	Bug Description	Severity <1=high; 2=medium; 3=low>
TC-LEX-OUD-004	BG-LEX-OUD-01	June 16, 2015	Run Time Error has occurred when scenario 2 strings are executed. (multiple word Problem)	1
TC-LEX-OUD-013	BG-LEX-OUD-02	June 16, 2015	Error: "Word not Found" for the string اُڑناآب	1
	BG-LEX-OUD-03	June 16, 2015	Run Time Error has occurred when scenario 1,2,3,4 strings are executed. (multiple word Problem)	1
TC-LEX-OUD-014	BG-LEX-OUD-04	June 16, 2015	Run Time Error has occurred when scenario 1, 2 strings are executed. (multiple word Problem)	1
TC-LEX-OUD-015	BG-LEX-OUD-05	June 16, 2015	Run Time Error has occurred when scenario 1 string is executed. (multiple word Problem)	1
TC-LEX-OUD-016	BG-LEX-OUD-06	June 16, 2015	For String 17 Error has occurred: "Word not Found".	1
TC-LEX-OUD-019	BG-LEX-OUD-07	June 16, 2015	Error has occurred: "Word not Found" for all strings.	1

TC-LEX-OUD-051	BG-LEX-OUD-08	June 17, 2015	Error: "Word not Found" for the string اُڑناآب	1
	BG-LEX-OUD-09	June 17, 2015	Run Time Error has occurred when scenario 1,2,3,4 strings are executed. (multiple word Problem)	1
TC-LEX-OUD-052	BG-LEX-OUD-10	June 17, 2015	Run Time Error has occurred when scenario 1, 2 strings are executed. (multiple word Problem)	1
TC-LEX-OUD-054	BG-LEX-OUD-11	June 17, 2015	For String 17 Error has occurred: "Word not Found".	1
TC-LEX-OUD-057	BG-LEX-OUD-12	June 17, 2015	Error has occurred: "Word not Found" for all strings.	1
TC-LEX-OUD-060	BG-LEX-OUD-13	June 17, 2015	Run Time Error has occurred when scenario 1 string 2 is executed. (multiple word Problem)	1
TC-LEX-OUD-061	BG-LEX-OUD-14	June 17, 2015	Error: It shows the list of similar words instead of detail of words. (For scenario 3 & 4 strings)	2
	BG-LEX-OUD-15	June 17, 2015	Run Time Error has occurred for scenario 5 string 1. Also see comments of this test case. (multiple word Problem)	1
TC-LEX-OUD-064	BG-LEX-OUD-16	June 20, 2015	Missing words error.	2
TC-LEX-OUD-067	BG-LEX-OUD-17	June 20, 2015	It does not recognise the single quote in the string that it belongs to English or not. So Prompt's wrong message.	1
TC-LEX-OUD-069	BG-LEX-OUD-18	June 20, 2015	It does not normalize single quote and apostrophe Properly.	1
TC-LEX-OUD-078	BG-LEX-OUD-19	June 20, 2015	Run time error. (Multiple words error.)	1
TC-LEX-OUD-301	BG-LEX-OUD-20	June 20, 2015	Symbols & Terminologies are now in help drop down	2
	BG-LEX-OUD-21	June 20, 2015	Help Link is not highlighted when we are on the page of Symbols & terminologies	2
TC-LEX-OUD-303	BG-LEX-OUD-22	June 20, 2015	“املاکےلیےراہنمائی ” is the missing Link in the help menu.	3
General Error	BG-LEX-OUD-23	June 20, 2015	Unusual characters are displayed e.g.ɑf.t̪ɑ.bi’.õ , ɑf.t̪ɑ’.bi ….	3
TC-LEX-OUD-086	BG-LEX-OUD-24	June 20, 2015	Not sorted according to Urdu Collation Sequence.	2

VII. Acknowledgements

I would like to thank my father for motivating me to work hard.

References References Referencias

1. Mr. Shakeel Nasir.OUD- Online Urdu Dictionary. Centre for Research in Urdu Language Processing, National University of Computer & Emerging Sciences-FAST. http://www.crulp.org/oud/default.aspx.
2. Doaa Nabil, Abeer Mosad, Hesham A. Hefny. Web-Based Applications quality factors: A survey and a proposed conceptual model. Egyptian Informatics Journal. 2011; 12(3): 211-217.
3. Basu, Anirban. Software Quality Assurance, Testing And Metrics.PHI Learning Private Limited; 2015.
4. Daniel Wollschlaeger, Heiko Karle.Using the DVHmetrics web application. 2015;https://cran.r-project.org/web/packages/DVHmetrics/vignettes/DVHshiny.pdf.
5. Imran Akhtar Khan and Roopa Singh. Quality Assurance and Integration Testing Aspects in Web Based Applications. International Journal of Computer Science, Engineering and Applications. 2012; 2(3):109-116.
6. Hari Sankar Chaini, Dr. Sateesh Kumar Pradhan. An Approach of Quality Assurance in Web Application. International Journal of Emerging Technology and Advanced Engineering. 2012; 2(8):130-133.
7. Shazia Arshad. Software Design Quality Metrics For Web Based Systems. Department of Computer Science and Engineering,University of Engineering and chnology. 2010;http://eprints.hec.gov.pk/9645/.

8. Kerry Rodden, Hilary Hutchinson, and Xin Fu. Measuring the User Experience on a Large Scale: User-Centered Metrics for Web Applications. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.2010; 2395-2398.
9. Babak Akhgar, Hamid R. Arabnia.Emerging Trends in ICT Security. Morgan Kaufmann Publishers Inc. San Francisco, CA, USA;2013
10. Rodrigo Elia Assad, Tarciana Katter, Felipe Silva Ferraz, Leopoldo Pires Ferreira, Silvio Romeiro Lemos Meira. Security Quality Assurance on Web-based Application Through SecurityRequirements Tests.Fifth International Conference on Software Engineering Advances IEEE.2010; 272-277.
11. Marianne Busch, Nora Koch, Santiago Suppan. Modeling Security Features of Web Applications.Springer International Publishing Switzerland. 2014; 119-139.
12. Asadullah Shaikh, Shccraz Ali, Nasrullah Memon, Panagiotis Karampelas.SOA Security Aspects in Web-based Architectural Design. Springer-Verlag Wien. 2010; 415-430.
13. Christoph Hochreiner, Zhendong Ma, Peter Kieseberg, Sebastian Schrittwieser, Edgar Weippl. Using Model Driven Security Approaches in Web Application Development. Springer Berlin Heidelberg. 2014; 419-431.
14. Prof. Dr. David Basin, Dr. Patrick Schaller, Michael Schläpfer. Web Application Security. Springer Berlin Heidelberg. 2011; 81-101.

This page is intentionally left blank

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 15 Issue 7 Version 1.0 Year 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Smart Acknowledgement Distributed Channel Access Scheme for TCP in Manets

By D. Sunitha, Dr. A. Nagaraju & Dr.G.Narsimha
Kamala Institute of Technology & Science, India

Abstract- TCP upon wireless networks is most challenging issue because of random losses and ACK interference. Also, TCP suffers from performance declination in terms of creating delay and overhead in network because of poor characteristics of wireless channel. In order to overcome these issues, we proposed a Smart Acknowledgement Distributed Channel Access (SADCA) scheme for TCP in MANETs. In the proposed scheme, first a separate Access Category (AC) for data less TCP acknowledgement packets is used and then it is assigned with highest priority. In this way, delay during transmission of packet can be reduced and also packet can be acknowledged immediately. Also, to increase the performance, delay window size can be adjusted by considering the parameters such as transmission rate, number of hops, and channel occupied ratio (COR). Hence the proposed scheme helps to avoid any kind of delay and overhead for sending TCP acknowledgement.

Keywords: distributed channel access; access category; TCP smart acknowledgement; manets.

GJCST-E Classification : C.2.5 C.2.1

SMARTACKNOWLEDGEMENTDISTRIBUTEDCHANNELACCESSSCHEMEFORTCPINMANETS

Strictly as per the compliance and regulations of:

Smart Acknowledgement Distributed Channel Access Scheme for TCP in Manets

D.Sunitha [α], Dr. A. Nagaraju [σ] & Dr.G.Narsimha [ρ]

Abstract- TCP upon wireless networks is most challenging issue because of random losses and ACK interference. Also, TCP suffers from performance declination in terms of creating delay and overhead in network because of poor characteristics of wireless channel. In order to overcome these issues, we proposed a Smart Acknowledgement Distributed Channel Access (SADCA) scheme for TCP in MANETs. In the proposed scheme, first a separate Access Category (AC) for data less TCP acknowledgement packets is used and then it is assigned with highest priority. In this way, delay during transmission of packet can be reduced and also packet can be acknowledged immediately. Also, to increase the performance, delay window size can be adjusted by considering the parameters such as transmission rate, number of hops, and channel occupied ratio (COR). Hence the proposed scheme helps to avoid any kind of delay and overhead for sending TCP acknowledgement.

keywords: distributed channel access; access category; TCP smart acknowledgement; manets.

I. Introduction

Mobile Ad-hoc Network(MANET) is an autonomous infrastructure-less system with wireless links connecting mobile nodes each operating as an end system as well as a router to forward packets and are free to move and form a network without any base stations. As mobile nodes communication is faster, it has a wide application in military applications, emergent operations, personal electronic device networking, and civilian applications like an ad-hoc meeting or an ad-hoc classroom. MANET's special characteristics like dynamic topologies, bandwidth constrained, variable capacity links, energy constrained operation, limited physical security make it susceptible to various attacks. In addition, jamming occurs in unreliable wireless links and eavesdropping due to their inherent broa dcast nature. Mobile devices' bandwidth, computing power, as well as battery power constraints causes application-specific trade-offs between devices' security and resource consumption. Behavior anomalies like advertising bogus routes are difficult to detect due to mobility[1].

The Transmission Control Protocol (TCP), the most commonly used reliable transport protocol in the internet, provide end-to-end reliable transmission as well as fair congestion control so as to share network resources efficiently[2]. Congestion control is a necessity for MANET since it operates in bandwidth constrained conditions.

TCP, in today's internet has poor performance and in MANETs is worsen by contention with increasing UDP-based high priority multimedia traffic and the class differentiation introduced in current QoS protocols, which results into TCP starvation and increased spurious timeouts [3]. The TCP usage over wireless networks rise to problems due to the different characteristics of wireless links with respect to wired ones, in terms of less reliability and time-variant behavior, fading / shadowing problems, node mobility, hand-offs, limited available bandwidth and large RTTs[5]. TCP performs reliably in traditional wired and stationary networks, but network congestion induces losses. Moreover, if the router waiting queues are full or nearly full, the packets received are dropped, thereby wired network losses are viewed as an indication of congestion. But in wireless networks the losses occur frequently for various causes such as interference, node mobility or poor link quality.

In MANETs, data transmission failures due to node mobility, interference, poor link quality, etc lead often to the congestion control activation by TCP protocol unnecessarily which degrades the performance of TCP in MANETs [2, 4,6].

The TCP reliability guarantees, TCP sender will forward each packet issued by it to the addressee node by a system of acknowledgements [4]. In TCP protocol, cumulative acknowledgements (ACKs) are sent by the TCP receiver for successfully received segments so as to let the TCP sender to find out the segments which have successfully received. The TCP sender determines the loss of packet either by several duplicate ACKs arrival, triggering a fast retransmission, or by the absence of an ACK for a timeout interval, thereby the TCP retransmits the lost packets, and simultaneously invokes congestion control by reducing its congestion window size and backing off its retransmission time for compensating packet losses. These reduce the level of congestion on the intermediate links [7].

The TCP Acknowledgements may return collide with their corresponding data packets in particular if the number of network nodes becomes vital. Such a large

Author α : Asst. Prof., Kamala Institute of Technology & Science, Singapur, Huzurabad, Telangana, India.
e-mail: dodda_sunitha@yahoo.co.in
Author σ : Asst. Prof, Central University of Rajastan, India.
e-mail: nagaraju@curaj.ac.in
Author ρ : Assoc. Prof. JNTU, Hyderabad, India.
e-mail: narsimha06@gmail.com

number of TCP ACK packets come into contention with TCP packets leads to intra-flow contention [4].

In our previous work [18], a cross-layer based approach for improving TCP performance in Multihop Mobile Ad-hoc Networks (MANETs) is proposed. The proposed mechanism triggers congestion whenever the channel occupied ratio (COR) reaches a maximum threshold value and the received signal strength is less than a minimum threshold value. Following it, congestion control scheme controls the data sending rate of the sender by determining available bandwidth, delay of its link and COR. Further, a fair resource allocation scheme is put forwarded.

As an extension to this work, we propose to design a smart acknowledgement distributed channel access scheme for TCP in order to reduce the delay and overhead of sending TCP acknowledgements.

II. Literature Review

Chien-Chia Chen et al [2] presented Combo Coding, a novel coding scheme combining intra- and inter-flow coding and a novel loss adaptation algorithm was featured. Combo Coding decreases the data and ACKs' interference within a TCP session taking advantage of the benefits of both types of codes, and also robustness to high link losses is exhibited. 2 Mbps good put is achieved by Combo Coding successfully with 30% per link packet loss rate; whereas TCP-New Reno with no coding delivers only 200 Kbps. Combo Coding over 2 paths provides a lower good put than that over a single path due to a higher overhead due to extra contentions as in the 20s–50s interval.

Sofiane Hamrioui et al [4] suggested an improvement of the Transmission Control Protocol (TCP), called Improvement of the Acknowledgement mechanism of TCP (IA-TCP), for MANET's better performance. Based on number of nodes, mobility and the communication distance between these nodes, IA-TCP delays TCP's acknowledgements packets. However, only throughput and end-to-end delay parameters are concerned. However, there is degradation of the TCP parameters performance.

Mohammad Amin Kheirandish Fard et al [10] proposed an end-to-end sender-side approach classifying congestion loss, wireless channel loss and link failure loss by queue usage estimation. Queue usage is calculated using relative One-way Trip Time.

Congestion loss is estimated using packet losses with queue usage rate greater than predefined threshold whereas non-congestion loss is when queue usage is less than threshold. Non congestion loss recognized by three duplicate ack labels loss caused by wireless channel error as it indicate the route existence between communicating end point that duplicate ACKs moved along.

Deguang Le et al [11] proposed a new cross-layer approach introducing a mobility detection element in the network layer to communicate with the transport layer for optimizing TCP operations. This approach preserves the end to end TCP semantics since end point changes are only made. Unlike other networks utilizing either transport or network layer alone without much cross-layer cooperation, this approach enable mobility information in TCP. However, RTO is reduced significantly compared to the standard TCP/MIPv6 as soon as the handover termination.

Consolee Mbarushimana et al [12] proposed a novel TCP-friendly scheme, IEDCA, for enhancing IEEE 802.11e EDCA mechanism by assigning the highest priority to TCP acknowledgement packets. The proposed scheme improves TCP performance significantly while having very negligible effects on voice traffic. However, the voice traffic dropped by buffer overflow or when the retry threshold is exceeded is higher in EDCA.

Toktam Mahmoodi et al [13] presented and assessed a cross-layer solution for a node for faster adaption of lower-layer characteristics like the coding rate and local ARQ retransmissions threshold according to the detected TCP flavor, so as to optimize the end-to-end performance of the download for that utilized flavor. The proposed scheme has considerable potential to improve the overall download throughput, without burdening the server and requiring no changes to existing TCP implementations. However, end-to-end throughput decreases with increasing propagation distance.

Myungjin Lee et al [14] proposed a path recovery notification (TCP–PRN) mechanism for avoiding performance degradation while handoff. Despite of being attained performance improvement while handoff, Freeze-TCP deployment in real environment is difficult due to obstacles in detecting accurate handoff time and the vulnerability of high variation in the round trip time (RTT). The proposed protocol restore congestion window avoiding it to reduce or immediately initiate slow start algorithm to recover lost packets. However, the handoff prediction is difficult and the variation of RTT is higher.

Ammar Mohammed Al-Jubari and Mohamed Othman [15] proposed a new delay-ACK algorithm for TCP performance enhancement over multi-hop wireless networks. According to factors like TCP startup phase, transmission rate, packet loss event, and number of hops, the optimal delayed ACK window is achieved dynamically as like before. The dynamic adaptive strategy's objective is enabling TCP receiver to adjust itself in terms of the data to ACK ratio. The scheme enhances TCP performance, attaining up to 233 % performance gain, over multi-hop wireless networks, compared to the regular TCP. However, the burst transmission occurs at the sender triggered by delayed

ACK. The burstiness increases the packet loss and potentially affects TCP performance.

III. Proposed Solution

a) Overview

The delay in packet transmission leads to loss of packet as well as throughput degradation. Hence we use a separate access category for data less TCP acknowledgement packets and assumed higher priority to them [12]. Hence delay in packet transmission can be reduced and packets are acknowledged instantaneously. Here higher congestion window value is attained than by TCP over Enhanced Distributed Channel Access (EDCA). Further improvements can be made by adjusting the delay window size by considering channel conditions like transmission rate, slow start phase, number of hops and packet lost event [15]. Here the number of acknowledgement packets can be reduced by generating the acknowledgement packets after attaining optimal dynamic delay window. Therefore receiver can adapt according to various delays.

b) Estimation of Metrics

i. *Probability of Successful Transmission :*

Most of the previous studies propose the probability of successful transmission based on analytical skills to compute delay and throughput that can be attained by different traffic categories in IEEE 802.11e for which they mainly considered Markov model. In this type of model successful transmission is given as below:

$$\gamma = \frac{2}{1+V+pV\sum_{i=0}^{n-1}(2p)^i} \qquad (1)$$

V represents initial contention window during backoff stage, p represents the conditional collision probability, and n represents maximum backoff stage. Also the transmission probability γ_k of a station of Access Category (AC) k can be given as below:

$$\gamma_k = \frac{2}{1+V_k+p_kV_k\sum_{i=0}^{n_k-1}(2p_k)^i} \qquad (2)$$

Based on above equation, similar expression can be obtained for throughput T_k which is attainable by an access category k as below

$$T_k = \frac{n_k\gamma_k(l-p_k)l}{p(t)H_{(t)}+p(c)H_{(s)}+p(e)\,\phi} \qquad (3)$$

Where l represents average transmission time of payload for access category 'k'. p(t), p(c) and p(e) are the probabilities of a slot time contains successful transmission, collision, and channel being idle respectively. H(s), H(t) and ϕ represents average slot length of successful transmission, collision and channel being inactive respectively. From the above expressions, it can be observed that probability of successful transmission for any AC is inversely proportional to contention window V. Hence station with traffic in high priority AC will have low values of V which in turn will have higher chance of transmitting their data than stations with best effort and will have better throughput. But this case is not applicable for TCP traffic. For TCP traffic, a packet is considered to be successfully transmitted in case TCP ACK is received by the sender before the retransmission time is over. Based on the probability idea of successful transmission given by equation (2), successful transmission probability in case of TCP traffic is a combination of probability of successfully transmitted data packet as well as probability of successfully received ACK packet. Hence, for TCP traffic belonging to AC1, probability of successful transmission can be given as below:

$$\boldsymbol{\gamma}_{\mathrm{TCP}} = \frac{4}{\left\{1+V_1+p_1V_1\sum_{i=0}^{n_1-1}(2p_i)^i\right\}^2} \qquad (4)$$

Here assume that data and ACK have the same transmission probability, since they belong to the same access category and moreover delayed ACK option is not used. Hence TCP throughput is different from any other best attempt throughput which is accessible by equation (3), as it depends on the value γTCP which is given in the equation (4)

ii. *Channel Occupied Ratio (COR)*

COR is defined as the ratio of total lengths of busy periods to the total transmission time. Consider T_T denotes the total transmission time and T_b represents total length of busy periods. Hence COR can be given as below:

$$COR = \frac{T_b}{T_T} \qquad (5)$$

By considering channel utilization factor, a threshold value Th_{COR} , it can be given as below:

$$COR \approx C_U(COR \leq Th_{COR}) \qquad (6)$$

Where, C_U denotes channel utilization factor and it is the measure of ratio of channel busyness time for successful transmissions to the total time T_T.

c) Smart Acknowledgement Distributed Channel Access Scheme

This section describes the proposed Smart Acknowledgement Distributed Channel Access (SADCA). The main aim of the proposed technique is to maximize the throughput without creating any delay in the network.

In this technique, an additional fifth access category saved for data less TCP ACK is defined. This new AC is assigned with highest priority. By placing data less TCP ACKs in top priority access category, probability of transmitting them on time is also maximized. Since the TCP ACK transmission probability tends to 1, transmission probability of TCP traffic can be expressed by equation (2). In similar way, the possible TCP throughput can be obtained by equation(3) with the exception that H_s increases by the value equal to time required to transfer both TCP ACK as well as MAC control packets that go along with it. By utilizing this method, the probability that all the TCP packets transmitted get acknowledged are increased. The underlying principle of this method make use of transport layer to control the volume of TCP ACKs on the channel. The volume of TCP ACKs permitted on the channel matches the volume of TCP data which is successfully transmitted and it is independent of the type of other traffic struggling for the same medium. To avoid any kind of congestion due to retransmission COR is validated inside the network using equation (5) and (6), if in case the delay due to congestion is found.

The implementation of the SADCA can be explained in steps as below:

Step 1 : In the first step, type of service (ToS) is usually applied at the application layer, however TCP ACKs originate from the transport layer, hence transport layer is responsible for assigning a proper ToS to them.

Step 2 : Since transport layer automatically assign the best effort ToS to TCP ACKs, a different ToS need to be assigned to them to distinguish them from best effort traffic.

Step 3 : To make the process simple, ToS value (224) is assigned to the data less TCP ACK at the transport layer when they are about to sent to the lower layer.

Step 4 : The MAC layer describes 8 user priority levels which are used to arrange the different data packets into different ACs.

Step 5 : By considering 224 as their transport layer ToS, TCP ACK will be allocated to the user 7.

Step 6 : Also a fifth AC is defined corresponding to MAC user priority value of 7 and hence collect the TCP ACKs.

The mapping of client priority (CP) to AC in SADCA is shown in Table 1. Hence an additional traffic queue is obtained in SADCA as shown in Fig. 1. The proposed aim is to allow TCP ACKs priority to the medium. After that priority is assigned to the new AC having smaller values of AIFS, CWmin and CWmax compared to the existing higher priority voice traffic as shown in Table 2.

Table 1 : Client Priority for Mapping in SADCA

Client Priority(CP)	Access Category(AC)	Designation
1	0	Background
2	0	Background
0	1	Best Effort
3	1	Best Effort
4	2	Video
5	2	Video
6	3	Voice
7	4	TCP ACK
8	1	COR

Table 2 : Medium Access Parameters for Different ACs in SADCA

AC	CW_{mi}	CW_{max}	AIFSN	$TXOP_{limit}$
Voice	7	15	2	3264
Video	15	31	2	6016
Best Effort	31	1023	3	0
Backgroun	31	1023	7	3264
TCP ACK	3	7	1	3264

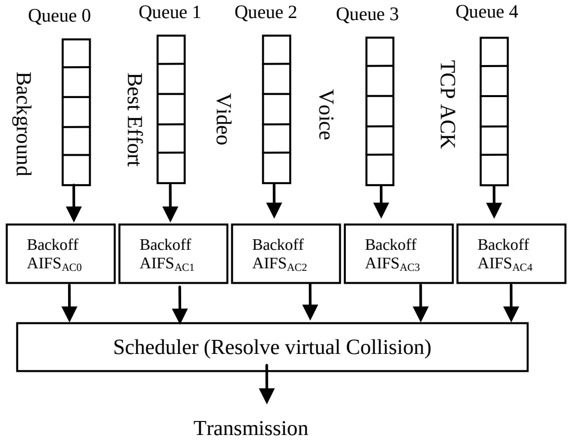


Fig. 1: Node within Transmission Range with Multiple priority queues in SADCA

The improvement in the proposed technique can be shown with the following example:

In case, TCP ACK is produced at the same time as the voice traffic, then station T_S gains the medium contention because these TCP ACKs are in an AC with higher priority than voice. Hence it can be said that T_S have more chance to transmit the TCP ACK before timeout and hence avoid the retransmission at the source. If the TCP ACK is generated before timeout, and then it avoids any kind of retransmission at the source.

Also if TCP ACK is generated after the VoIP conversation started, then it will have a good opportunity to compete for the medium at the end of the next TXOP of the VoIP stations. Hence it can be said that, there is a high chance that ACK will be received within the RTO limit. Also retransmission can be avoided.

IV. Simulation Results

a) Simulation Setup

NS-2 simulator is used to simulate the Smart Acknowledgement Distributed Channel Access scheme for TCP (SADCA-TCP) protocol. In our simulation, the channel capacity of all mobile hosts is set to 2 Mbps. Distributed coordination function (DCF) of IEEE 802.11 for wireless LANs is used as the MAC layer protocol. It has the functionality to notify the network layer about link breakage. The following metrics are used to compare SADCA-TCP with standard simple TCP protocol.

Packet delivery ratio: It is defined as the ratio of the total number of packets received at the destination over the total number of packets transmitted.

Average end-to-end delay: The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.

Throughput: It is the total bandwidth received at the destination measured in Mb/sec.

b) Static Line Topology

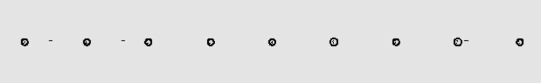


Fig. 2 : Static Line Topology

In the static line topology, 9 static nodes are arranged as a line topology in a 1700 meter x 300 meter region as shown in Fig. 2. All nodes have the same transmission range of 250 meters. All the data flows are set as long follows.

The simulation settings and parameters are summarized in Table 3

Table 3 : Simulation settings for Static Topology

No. of Nodes	9
Area Size	1700 X 300
Mac	8021.11
Radio Range	250m
Simulation Time	300 sec
Traffic Source	FTP
Packet Size	1000 bytes
No. of Flows	1 to 8
Routing Protocol	AODV

The simulation results are given below:

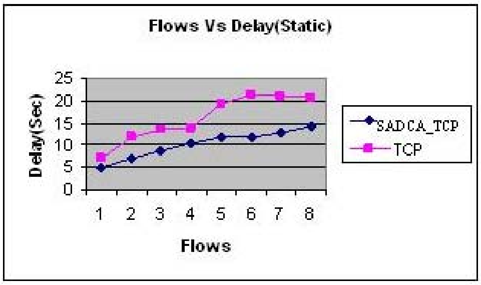


Fig. 3: Flows Vs Delay

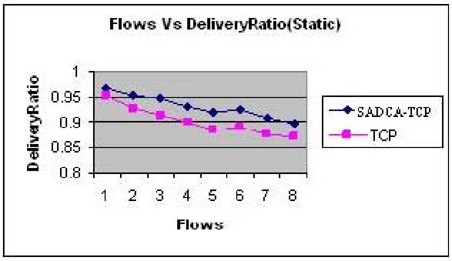


Fig. 4 : Flows Vs Delivery Ratio

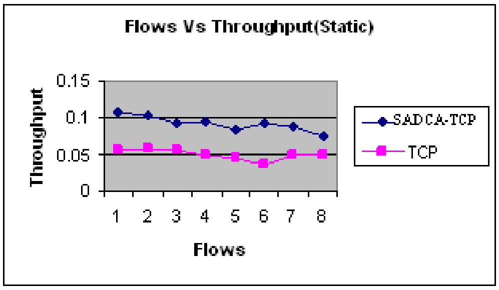


Fig. 5 : Flows Vs Throughput

Fig. 3 shows the delay of SADCA-TCP and TCP techniques for different number of flows scenario. We can conclude that the delay of SADCA-TCP has 35% of less than TCP.

Fig. 4 shows the delivery ratio of SADCA-TCP and TCP techniques for different number of flows scenario. We can conclude that the delivery ratio of SADCA-TCP has 3% of higher than TCP.

Fig. 5 shows the throughput of SADCA-TCP and TCP techniques for different number of flows scenario. We can conclude that the throughput of SADCA-TCP has 45% of higher than TCP.

c) Dynamic Random Topology

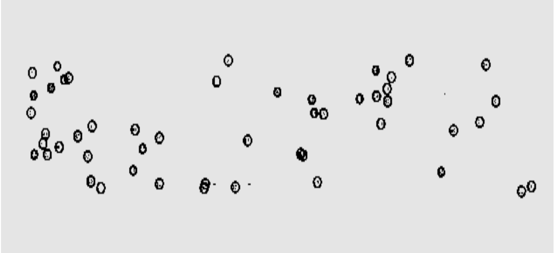


Fig. 6 : Dynamic Random Topology

In the dynamic random topology, 50 mobile nodes are deployed randomly in a 1500 meter x 300 meter region as shown in Fig. 6. All nodes have the same transmission range of 250 meters. The random way point model of ns-2 is used as the mobility model in which the pause time of the node is 5 seconds and speed is 10 m/s. There are 10 traffic flows between different set of source and destination pairs.

The simulation settings and parameters are summarized in Table 4.

Table 4 : Simulation settings for Dynamic Topology

No. of Nodes	50
Area Size	1500 X 300
Mac	8021.11
Radio Range	250m
Simulation Time	300 sec
Pause time	5 seconds
Speed	10 m/s
Traffic Source	FTP
Packet Size	512 bytes
No. of Flows	1 to 10
Routing Protocol	AODV

The simulation results are given below:

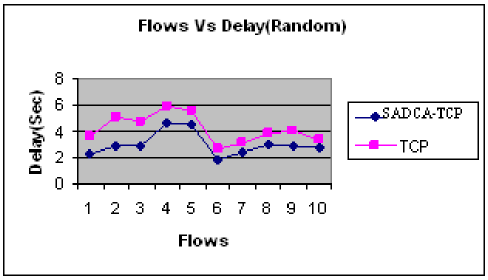


Fig. 7 : Flows Vs Delay

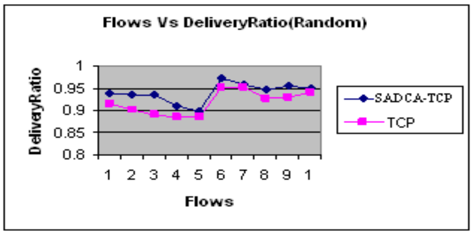


Fig. 8 : Flows Vs Delivery Ratio

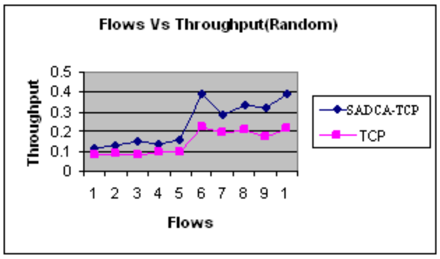


Fig. 9 : Flows Vs Throughput

Fig.7 shows the delay of SADCA-TCP and TCP techniques for different number of flows scenario. We can conclude that the delay of SADCA-TCP has 28% of less than TCP.

Fig.8 shows the delivery ratio of SADCA-TCP and TCP techniques for different number of flows scenario. We can conclude that the delivery ratio of SADCA-TCP has 2% of higher than TCP.

Fig.9 shows the throughput of SADCA-TCP and TCP techniques for different number of flows scenario. We can conclude that the throughput of SADCA-TCP has 37% of higher than TCP.

V. Conclusion

In this paper we have proposed a Smart Acknowledgement Distributed Channel Access (SADCA) scheme for TCP in MANETs. In the proposed scheme, first a separate access category for data less TCP acknowledgement packets is used and also it is assigned with highest priority. As the TCP ACK is assigned with new AC with highest priority, it has maximum probability of successful transmission by making efficient utilization of contention window during backoff stage. In this way, delay during transmission of packet can be reduced and also packet can be acknowledged immediately. Also, to increase the performance, delay window size can be adjusted for optimization purpose by considering the parameters such as transmission rate, number of hops, and congestion occupied ratio (COR). Hence the proposed scheme helps to avoid any kind of delay and overhead for sending TCP acknowledgement

References References References

1. Junhai Luo, Xue Liu and Mingyu Fan, "A trust model based on fuzzy recommendation for mobile ad-hoc networks", Computer Networks, 2009, pp. 2396–2407.
2. Chien-Chia Chen, Clifford Chen, Soon Y. Oh, Joon-Sang Park, Mario Gerla and M.Y. Sanadidi, "Combo Coding: Combined intra-/inter-flow network coding for TCP over disruptive MANETs", Journal of Advanced Research, 2011, pp. 241–252.
3. Consolée Mbarushimana and Ali Shahrabi, "E-TCP: Enhanced TCP for IEEE802.11e Mobile Ad Hoc Networks", 15th International Conference on Parallel and Distributed Systems, 2009.
4. Sofiane Hamrioui, Mustapha Lalam and Pascal Lorenz, "IA-TCP: Improving Acknowledgement Mechanism of TCP for better performance in MANET", International Journal on New Computer Architectures and Their Applications (IJNCAA), 2012, pp. 333-341.
5. Dzmitry Kliazovich and Fabrizio Granelli, "A Cross-layer Scheme for TCP Performance Improvement in Wireless LANs", IEEE Global Telecommunications Conference, GLOBECOM'04, Vol. 2, 2004.
6. Yassine Douga and Malika Bourenane, "A Cross layer solution to improve TCP performances in Ad hoc Wireless Networks", IEEE International Conference on Smart Communications in Network Technologies (SaCoNeT), Vol. 1, 2013.
7. Wenqing Ding and Abbas Jamalipour, "Delay Performance of the New Explicit Loss Notification TCP Technique for Wireless Networks", IEEE Global

Telecommunications Conference, GLOBECOM'01, Vol. 6, 2001.

8. Ruy de Oliveira and Torsten Braun, “A Smart TCP Acknowledgement Approach for Multihop Wireless Networks”, IEEE Transactions On Mobile Computing, Vol. 6, No. 2, February 2007.
9. Hongqiang Zhai, Xiang Chen, and Yuguang Fang, “Improving Transport Layer Performance in Multihop Ad Hoc Networks by Exploiting MAC Layer Information”, IEEE Transactions On Wireless Communications, Vol. 6, No. 5, May 2007.
10. Mohammad Amin Kheirandish Fard, Sasan Karamizadeh and Mohammad Aflaki, “Packet Loss Differentiation of TCP over Mobile Ad Hoc Network Using Queue Usage Estimation”, IEEE 3rd International Conference on Communication Software and Networks (ICCSN), Xi'an, 2011.
11. Deguang Le, Xiaoming Fu and Dieter Hogrefe, “A Cross-Layer Approach for Improving TCP Performance in Mobile Environments", Wireless Personal Communications, Feb 2010, Vol. 52, No. 3, pp. 669-692.
12. Consolee Mbarushimana, Ali Shahrabi and Tom Buggy, “A Cross-Layer Support for TCP Enhancement in QoS-Aware Mobile Ad Hoc Networks”, In proceeding of the 11th International Symposium on Modeling Analysis and Simulation of Wireless and Mobile Systems, MSWiM, Vancouver, British Columbia, Canada, October 27-31, 2008.
13. Toktam Mahmoodi, Oliver Holland, Vasilis Friderikos and Hamid Aghvami, “Cross-Layer Optimization of the Link-Layer based on the Detected TCP Flavor", IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC, Cannes, 2008.
14. Myungjin Lee, Moonsoo Kang, Myungchul Kim and Jeonghoon Mo, “A cross-layer approach for TCP optimization over wireless and mobile networks”, Computer Communications, pp. 2669–2675, 2008.
15. Ammar Mohammed Al-Jubari and Mohamed Othman, “A New Delayed ACK Strategy for TCP in Multi-hop Wireless Networks”, Information Technology International Symposium (ITSim), Kuala Lumpur, Vol. 2, 2010.
16. Jiwei Chen, Yeng Zhong Lee, Mario Gerla and M.Y. Sanadidi, “TCP with Delayed Ack for Wireless Networks”, 3rd Broadband Communications, Networks and Systems BROADNETS, 2006.
17. Sara Landström and Lars-Åke Larzon, “Reducing the TCP Acknowledgement Frequency", ACM SIGCOMM Computer Communication Review, pp.5-16.
18. D.Sunitha, A.Nagaraju, G.Narsimha, “ A cross-layer approach for congestion control in Multi hop Mobile Ad hoc Networks” Computing for Sustainable Global Development (INDIACom), 2014 IEEE Xplore March 2014, pp54-60
19. S. Subburamm and P. Sheik Abdul Khader, “Efficient Broadcasting using Preventive Congestion Mechanism in Mobile ad Hoc Network”, European Journal of Scientific Research, Vol.83, No.2, pp.302-313, 2012.
20. Rajkumar, G. and K. Duraiswamy, “A Fault Tolerant Congestion Aware Routing Protocol for Mobile Ad hoc Networks”, Journal of Computer Science, Vol.8, No.5, pp.673-680, 2012.
21. Ramachandra V.Pujeri and S.Sheeja, “Cross Layer based Congestion Control Scheme for Mobile Ad hoc Networks”, International Journal of Computer Applications, Vol.67, No.9, pp.61-63, 2013

This page is intentionally left blank

Global Journals Inc.

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 15 Issue 7 Version 1.0 Year 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Security Issues and Energy Consumption in Implementing Wireless Sensor Networks

By Sameer Alalawi & Zenon Chaczko

University of Technology, Australia

Abstract- The Internet has become an indispensable means of sourcing and storing information. In the future, the Internet will be used to control objects, not just information. This raises the issue of security. In the case of wireless sensor networks, the main challenge will be to provide secure lines of communication between devices on the same network.

Keywords: *WSNs; attacks; threats; sinkhole attack; hello flood attack.*

GJCST-E Classification : *C.2.1 D.4.6 C.2.5*

Security Issues and Energy Consumption in Implementing Wireless Sensor Networks

Sameer Alalawi [α] & Zenon Chaczko [σ]

Abstract- The Internet has become an indispensable means of sourcing and storing information. In the future, the Internet will be used to control objects, not just information. This raises the issue of security. In the case of wireless sensor networks, the main challenge will be to provide secure lines of communication between devices on the same network.

Keywords: WSNs; attacks; threats; sinkhole attack; hello flood attack.

I. Introduction

Sensors have been implemented to read information from physical devices in order to use this information for multiple purposes. Sensors convert analog signals to digital signals for processing and computation purposes. 'A sensor is a type of transducer that converts energy in the physical world into electrical energy that can be passed to a computing system or controller' (Dargie et al. 2010 p. 4). Furthermore, sensors have the ability to send and receive information to other sensors in the same area, creating a network between several sensors. This is called a wireless sensor network (WSN), which is 'a group of sensors cooperatively monitoring a large physical environment' (Dargie et al. 2010 p. 7). While a Wireless sensor network provides full controlling on devices by sending and receiving information between them, it requires strong security mechanisms against the threats of attackers. In this way, implementing wired security mechanisms in a WSN is an inefficient solution. Bashir & Hussain (2013) indicate that providing security protocols for WSNs is a big challenge due to the resource constraints of the WSN itself. Furthermore, Boukerch et al. (2007) point out that the reason of inefficiency of using the wired or wireless security mechanisms in a WSN is the CPU computations, delay constraints and the communications of applications that run on the top of that network. Applying traditional security mechanisms in WSNs increases the delay of transferring information and causes packets of information to go missing when transferring in WSN communication.

Network security requires four mechanisms in order to control the resources and keep these resources safe. These mechanisms are confidentiality, integrity, authentication and availability. Each mechanism requires certain protocols, which are working together to achieve these four security goals. The perfect solution to prevent attacks is to understand the behaviour of their threats and protect the resources against these attacks. Several papers explain threats to WSNs and classify them into more than one class. Tahir & Shah (2008) classify threats in WSNs into two classes. The first are mote class attackers, the second are laptop-class attackers. The attackers are further categorised into four dimensions: motive, determination, knowledge and resources. Threats in WSNs can also be categorized depending on the OSI model layers. This classification is useful in troubleshooting and maintenance purposes. In addition, the OSI model simplifies the detection of the attacking, which is the most difficult step to detect the threats. Sarma & Kar (2006) indicate some examples of threats, which relate to the OSI layers, such as the physical layer which is threatened by jamming and tampering, the data link layer which is threatened by the collision or exhaustion, and the network layer which is threatened by routing protocol. This report discusses some proposed solutions of the security mechanisms and provides the results of a simulation for sinkhole and hello flood attacks which WSNs are susceptible to. The first section provides background and reviews the threats in the WSN, the second section explains the method used to examine the behaviour of sensors under threat, the third section views the results of this simulation, the fourth section discusses the results of the simulation for examining the sinkhole and hello flood attacks and provides solutions to these threats.

II. Literature Review/Background

Several papers discuss the threats to WSNs as a big issue in creating a network design. Path et al. (2006) mention that most threats to WSNs are similar to those that threaten wireless networks, but some are specific to WSNs. However, the security solutions for wireless networks cannot be applied successfully to wireless sensor networks due to the architectural dissimilarities of these two networks. Tahir & Shah (2008) point out some common security threats, which attack sensor nodes in WSNs. The first threat is a sleep duration attack; this attack happens during the changing from active to sleep mode. The main purpose of this attack is to prevent sensor nodes from energy saving while it is in a sleep mode in order to reduce the power

Author α σ : Technical and Vocational Training Corporation (TVTC) KSA, University of Technology, Sydney (UTS).
e-mails: s.alshoikan@tvtc.gov.sa, Czenon.Chaczho@uts.edu.au

resources (Tahir & Shah 2008). Consequently, the attacker controls other sensors by International Journal of Industrial Electronics and Electrical Engineering, ISSN: 2347-6982 Volume-3, Issue-10, Oct. -2015 Security Issues And Energy Consumption In Implementing Wireless Sensor Networks 15 sending a request, which makes it appear as if the sensor is dead. Another threat is the sinkhole attack. The attacker in a sinkhole attack attracts all routing paths towards itself. Pathan, Lee & Hong (2006) indicate that some malicious nodes try to attract all the traffic in the sensor network. In a flooding based control, the attackers receive a request for routing and send it to the target node. Malicious nodes will be able to control the packets transferring between nodes, while it involves itself between them. The third threat to WSNs is the wormhole attack .The attacker in this threat records the packets at one of the locations and transfers these packets to another location. Tahir & Shah (2008) point out that this kind of threat gives the malicious nodes in the WSN the observation to attract the other nodes for routing. The sybil attack is another kind of threat to WSNs. This attack tries to tamper with the integrity of data in order to attack the distribution storage, routing protocol and data aggregation. This attack occurs by using fake locations of multiple identities. Consequently, the attacker will be located in multiple locations with different identities. The fifth threat is the hello flood attack; this attack uses hello packets as a sign to attack the sensor nodes. Hello flood attack is a laptop class (Tahir & Shah 2008). While the hello message is a crucial sign for establishing a successful communication between neighbours' nodes, the attacker who uses hello flood attack tries to announce itself to be one of the neighbours of other nodes in order to involve itself in the attacking network. Denial of service attack is also considered as one of the threats in network design. The main idea of this threat is that the attacker tries to exhaust all resources in the attacking network by sending a large number of unnecessary packets. Tahir & Shah (2008) discuss a kind of denial of service attacks called a jamming attack. A jamming attack tries to jam the communication between sensor nodes. Thus, these previous threats attack the software of nodes communication in the WSN considering on the routing protocols.

Some threats attack the hardware of sensors instead of software. Adnan, Yussoff & Hashim (2010) point out the physical prospective threats to WSNs, which is attacking the initial boot phase of the devices. Another threat is passive information gathering, which collects information from nodes, while the data is not encrypted. Tahir & Shah (2008) indicate that attackers can destroy sensors by extracting the physical location especially if the attacker is a laptop class. The authors recommend a combination between hardware security solutions with software security solutions in wireless sensor networks, to enhance the security level in the system.

III. Sinkhole Attack

A sinkhole attack targets the sink nodes in order to persuade all traffic through it for stealing the nodes' information. Hamedheidari & Rafeh (2013) indicate that the goal of a sinkhole attack is to change the routing paths from one area to another. In a WSN, creating sinkhole attacks is easy because the routing topology in this network is based on tree routing. Tree based routing topology increases the impact of malicious nodes, which are dependent on the number of uncompromised sensors. Hamedheidari & Rafeh (2013) explain the way of launching sinkhole attacks in distance vector routing protocol (AODV); this routing method depends on hop count to find the shortest path to the base station. The malicious node in this case sends a message to the sender telling it its path is the best and shortest path to the base station. Consequently, the attacker node collects all data coming through it. Furthermore, sinkhole attacks prevent the base station from getting correct data from neighbours (Sreelaja & Pai 2014). This is the result of persuading all routing paths neighbours to the attacking nodes. However, the detection of sinkhole attacking node is difficult because the attacker uses the right authentication of the normal sensor to establish a communication with neighbours. The attacker in a sinkhole threat can affect the sink node and establish the attack in two ways. The first type is malicious insider, while the second type is resourceful outsider. Shafiei et al. (2014) point out that the attacker uses a malicious node to start the attacking by deceiving neighbours that the compromised node is the best path to the base station. As the result of that, laptop class malicious node, which is equipped with high performance, leads the network route from the right paths to the malicious node path. The high performance malicious node may attract most surrounding nodes to the sinkhole (Shafiei et al. 2014). Furthermore, sinkhole may threaten by using a wormhole attack after capturing all packets from the sink nodes' neighbours and using a tunnel to transfer packets to the other nodes, which is colluded to the malicious node. The main job of the colluded node is sending messages to the base station. Shafiei et al. (2014) indicate that this attack prevents the sender from discovering any routing path except the tunnel, which leads to disruption of the network's functionality.

Several papers proposed means of how to detect and prevent a sinkhole attack. Sreelaja & Pai (2014) explain the swarm inelegance approach of sinkhole threats against hope count routing protocol. This approach detects the sinkhole attack in distance vector routing protocol using a slowly hop count monitoring and an alert method in order to generate the threat on detecting the sinkhole attack. On the other hand, Hamedheidari & Rafeh (2014) proposed a trust model to detect the attacking nodes and prevent the threats; this trust node uses three codes before establishing the communication between sensors. However, these approaches are inefficient in WSNs due to the mobility of nodes; which is the most important method for WSNs in distance vector International Journal of Industrial Electronics and Electrical Engineering, ISSN: 2347-6982 Volume-3, Issue-10, Oct.-2015 Security Issues And Energy Consumption In Implementing Wireless Sensor Networks 16 protocol. This is because the mobility of nodes may leave some nodes without covering of any agents; uncovered nodes are considered unreliable, which makes it possible for malicious nodes to attack this unreliable node (Hamedheidari & Rafeh 2014). However, Fessant et al. (2012) analyse two protocols that increase the network performance with the existence of the sinkhole attack. These protocols are ERSIST-1 and ERSIST-0. While ERSIST-0 prevents malicious nodes from lying about their advertised distance, ERSIST-1 stops the lying about their advertised distance.

IV. Simple Configuration Protocol (Resist 1)

This protocol uses the hello messages, which consist of epoch-tokens as a trust key to all neighbours. The sensor chooses one of the following when it receives the hello message:

1. If the epoch is new, that means it receives the current epoch and it has to send the next one to the shortest path.
2. If the epoch is already taken, the node updates itself and propagates a new hello message to the neighbours.

This protocol guarantees that the sinkhole attack forwards the messages without dropping the first epoch-token.

V. Complex Configuration Protocol (Resist 0)

This protocol uses the same of ERSIST-1 but the sensor challenges its parents before sending the hello messages by using public and private keys. This approach is useful while the malicious node does not have the private key of the sinkhole. Furthermore, dropping the packets does not succeed because neighbour nodes would not respond to the challenge if it does not match.

Fessant et al. (2012) indicate that signing the key is an issue in WSNs due to the lack of memory. However, there are several approaches that are proposed to design key management such as LEDs but they still need to be more efficient to work in WSNs.

VI. Hello Flood Attack in Wireless Sensor Networks

WSNs depend on certain protocols to manage the communication between nodes. Nodes in this network use hello packets in order to communicate with their neighbours and calculate the best path routing to the base station. However, the attackers use this protocol to threaten the network topology by introducing a malicious node to the other nodes in the range and spread its threat to the rest of the nodes in the attacked network. Hello flooding attack is designed to exploit the broadcasting nature of these protocols in order to convince a large group of nodes that the sender is a normal neighbour, by using a very high transmit power (Haghighi et al. 2011). A laptop class attacker could persuade all nodes in the network that the attacked node is a normal neighbour. In this way, the attacked node does not need to seem legal for the other nodes in order to attack the network because it can convince the other nodes to follow it by producing a high power signal for broadcasting. After attacking the target node, the attacker uses flooding to spread viruses via broadcast messages to all nodes in the network; " the hello flood attack uses a single hope broadcast to transmit the message to a large number of receivers" (Karlof et al. 2003 p. 302). Furthermore, laptop class uses the hello flood attack to disable the functionality of the target network by changing the power of transmit to reach the lowest value of broadcasting to the other neighbours after convincing these nodes. In this way, several efforts deliver some solutions for the hello flood attacking in a WSN. Karlof & Wagner (2003) point out that verifying the two ways links of every node is one of the solutions for defencing the hello flood attack. However, this solution is inefficient if the malicious node reduces a high power transmit for the other neighbour nodes, due to the high convince of the malicious node. Moreover, authentication is another solution for this issue by challenging all links around the nodes before accepting the hello message. While authentication prevents the hello flood from spreading due to the challenging methods, it does not prevent the compromised nodes from authenticating themselves to their neighbours in the network.

VII. Using Leach Protocol to Detect the Hello Flood Attack

LEACH (Low-Energy Adaptive Clustering Hierarchy) is a technology used for managing the hierarchy of the topology in a WSN. The main goal of LEACH protocol is allowing every node connected to the WSN to reach the base station (Magotra & Kumar 2014). LEACH groups nodes into several clusters; one of the nodes inside the cluster acts as a cluster head. Magotra & Kumar (2014) indicate that LEACH protocol uses random alternation of the nodes to be the cluster head; since the new cluster head takes its position, it sends new hello packets to all neighbours in its range.

Several studies use LEACH protocol to address the hello flood attack and prevent the threats presented by malicious nodes. Magotra & Kumar (2014) classify these studies into two groups; while the first group focuses on cryptographic-based approach, such as FLEACH, S-LEACH and sec-LEACH, the second group focuses on non-cryptographic based International Journal of Industrial Electronics and Electrical Engineering, ISSN: 2347-6982 Volume-3, Issue-10, Oct.-2015 Security Issues And Energy Consumption In Implementing Wireless Sensor Networks 17 approaches such as the single strength based detection approach.

The non-cluster head mode is a node without a cluster head agent in LEACH protocol, compares the RSS with the distance between non-CH and any elected CH node. Magotra & Kumar (2014) indicate that nodes whose RSS and distance in the same range are able to join the cluster head. The node calculates the distance to the cluster head depending on this formula:

$$Dis= \text{sqrt}\ [\text{sq}\ (x2 - x1) + \text{sq}\ (y2 - y1)]$$

Such as, x1 and y1 are the location of nodes receiving packets, x2 and y2 are the location of the cluster head, which is sent via hello packet; this calculation is for the sending and the receiving nodes.

VIII. Hello Flood Attack Detection

LEACH protocol focuses on changing the cluster head regularly to prevent the threats and improve the network performance. Magotra & Kumar (2014) proposed that this changing is based on two parameters. The first parameter focuses on the position of the nodes, while the second parameter focuses on the number random round of choosing a new cluster head in LEACH protocol.

- Attacking node position

It focuses on the nodes position and replaces the malicious node by using LEACH protocol. Three scenarios are used to replace the attacked node with a normal node.

➢ Detection time period: It is the average of time by the total number of nodes in the network in order to detect the malicious node.

➢ Energy required: It is the average of energy by the total number of nodes in the network in order to detect the malicious node.

➢ Communication: It is the number of test packets detecting, which is sent by the malicious node for creating the hello flooding attack.

Magotra & Kumar (2014) indicate that the communication is secure from the hello flooding attack while the test packets transferring between nodes is in the lowest average.

- Number of random rounds in LEACH

The changing of cluster head randomly and regularly between nodes, leads to understand the effect ofmalicious nodes. The result of that is increasing the performance of the WSN even when the nodes are affected by a hello flood attack. This is because the hello flood attack can be detected with low energy and in less time. A low rate of energy leads to increasing the network performance lifetime and detect the hello flood attack (Magotra & Kumar 2014).

IX. Research Methods

The method used for this research is a simulation, which simulates the behaviour of sensors in a WSN under attack. Wise-net simulation is implemented to simulate the communication between nodes in any environment. It helps WSNs designers to examine the routing paths between nodes in the network. We use this simulator to simulate the sensor behaviour under two kinds of attacks. These attacks are sinkhole attack and hello flood attack. The simulation provides several outputs for each test. This project focuses on the energy of the sensor before and after the attack.

X. Results

a) *Normal node*

The normal connection in figure 1 shows the way of routing protocol messages between nodes as well as the energy consumption, which is produced from the base station. Normally, the base station (sink node) provides energy to all sensors, which are located in the same area. Consequently, the sensors communicate with each other using the received energy from the base station. However, the messages transmission in normal nodes simulation records 91%, this percentage is reasonable enough to ensure perfect communication between nodes in the same cluster.

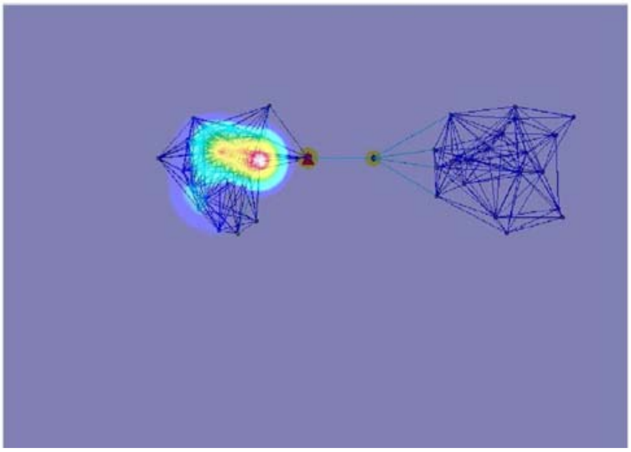


Figure 1: shows the normal energy of the node's connection Security Issues and Energy consumption in Implementing Wireless Sensor Networks November 3, 2014

b) Sinkhole attack nodes

Nodes under a sinkhole attack are unstable and dysfunctional due to the lack of providing the energy needed. Figure 3 shows the energy chart of nodes under a sinkhole attack. It shows losing of energy especially in the core of the network topology. This is because the malicious node tries to persuade all routing paths toward itself, which results in a confusion in sending and receiving information between nodes. For example, a normal node changes the routing request from the correct path to the wrong path by using a malicious node. This is because the International Journal of Industrial Electronics and Electrical Engineering, ISSN: 2347-6982 Volume-3, Issue-10, Oct.-2015 Security Issues And Energy Consumption In Implementing Wireless Sensor Networks 18 malicious node attracts nodes in that area that its path is the best path to the base station by using a highenergy output. Figure 3 shows that the transmission and routing feedback are dropped compared with the normal node's situation.

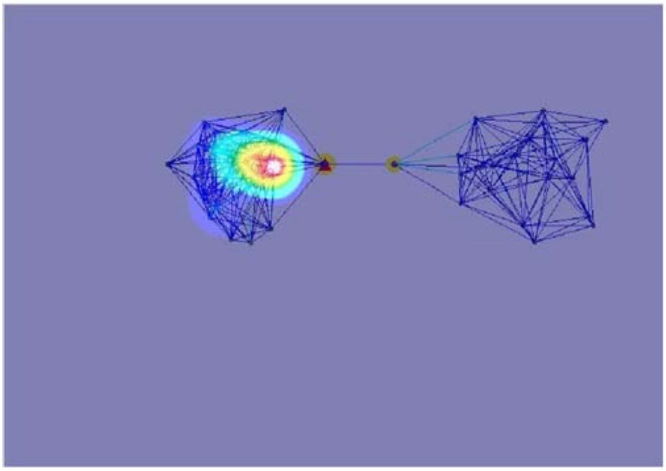


Figure 2 : shows the nodes energy under sinkhole attack

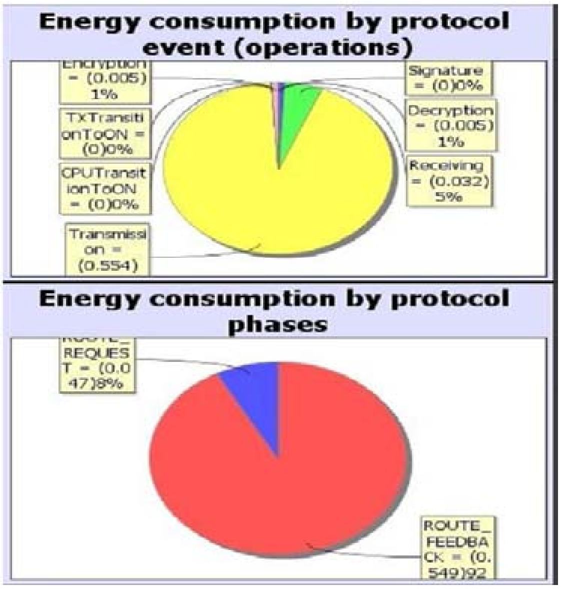


Figure 3 : shows a chart of energy consumption under sinkhole attack

Security Issues and Energy consumption in Implementing Wireless Sensor Networks November 3, 2014

c) Hello flood attack node

The malicious node in hello flood attack provides different mechanisms to the nodes in the network for attacking the network. Figure (4) shows that the energy distribution of sensors has changed due to the attacking. The malicious node in hello flood attack divides the energy consumption into two parts in this network. This is because the hello flood attack tries to separate the network then control each part separately in order to lose the energy of sensors. Figure 5 shows that the transmission between nodes under hello flood attack is decreasing compared with the normal nodes, but the route feedback is increased compared with nodes under sinkhole attack. This is because hello flood focuses on sending and receiving messages between nodes to persuade them that the malicious node is the best path to the base station.

XI. Routing Information

In this section the base station is chosen to examine the output of its routing information for all three types of connection; normal connection, sinkhole attack connection and hello flood attack connection. We examine all connection cases with 12 simulation nodes and 11 neighbours as shown in table (1). From the results we found that the energy in normal connection is the highest than all of the other connections; this is normal because the energy is distributed to all nodes equally. On the other hand, the number of messages received in hello flood attack connection is the highest number comparing with the other connections, due to the behaviour of the malicious node in this attack.

Connection	Number of nodes	Number of messages sent	Number of messages received	Neighbour/node	Total energy
Normal	42	86	1228	11	0.664
Sinkhole	42	80	1128	11	0.596
Hello flood	42	86	1278	11	0.651

XII. Discussion

From the results of these simulations we found that that the energy is changed consequently with the changing of node behaviour. These threats affect the network energy which leads to changing the correct routing path for sending and receiving the information in order to connect to the base station. While wireless security mechanisms defend against the threats and provide a good protection for the network design, these mechanisms in wireless sensor networks need to add some new features for sending and receiving information in a secure way. This is because the security mechanisms require memory and CPU for computation and finding results. In this area using routing protocol, which protects the communication between sensors nodes by adding a secure header for all packets transferring is one of the proposed solutions. On the other side, LEACH protocol is also a good method to secure a wireless sensor network, by changing the base station regularly to ensure that the attacked node is changing if it is affected by any threat. Furthermore, using 6LOW-PAN protocol with low power consumption in routing protocol is a part of this solution to prevent the lack of energy. However, these changes of nodes and routing methods need to be adjustable with the threats affecting the rank of sensors, this is because these changes lead to the weakening of the cryptographic solution.

XIII. Conclusion

WSNs are the basic technology for building networks of devices that can be controlled via the Internet. The sensor technology converts analog signals such as sound or light to digital signals for computation and International Journal of Industrial Electronics and Electrical Engineering, ISSN: 2347-6982 Volume-3, Issue-10, Oct.-2015 Security Issues And Energy Consumption In Implementing Wireless Sensor Networks 19 communication. The communication between sensors requires an efficient design to create a WSN topology. For example, using clusters to divide the sensor nodes into several parts in order to organize the network resources. This report has discussed some of the challenges for creating an efficient and reliable wireless sensor network by reviewing and discussing the security issues in implementing the topology of WSN design. From the examination of two kinds of attacks in WSNs, we found that the energy distribution of sensors is disrupted in consequence of the threat, which is caused by the malicious nodes. For example, the sinkhole attack tries to persuade all routing traffic toward itself in order to capture all information of nodes. This is because the attacker changes the energy power producer from the base station (sink-node) to the malicious node. Another example for examining the threat in a WSN is the hello flood attack. This attack uses the hello flood attack to send affected messages to its neighbours. From the simulation of hello flood attack, we found that the power consumption of the sensor in one cluster is divided into two parts, which allows the malicious node to control each part separately by dividing the power after attacking.

Several papers propose some mechanisms for implementing a secure WSN. LEACH protocol is one of these mechanisms, which considers in changing the base station regularly. While this mechanism solves some attacks and helps the network designers to create a secure WSN, it causes instability in the network in consequence of changing the routing methods. On the other hand, using an epoch-token as a trust key is another mechanism proposed to solve the security issue in wireless sensor network. This mechanism is successful in detecting the sinkhole attack, because it sends and receives the pre-shared key between the node and its base station. However, no paper until now has proposed how to detect the other threats, such as hello flood or denial of services using the epoch-token mechanism. All attacks focuses on the energy for persuading the other nodes that the malicious node is the best path to the base station. For that reason, implementing a trust model for energy with these mechanisms of security may solve that problem. For example, Use 6- LOWPAN routing protocol, which consumes low power in routing method between sensors, may leads to stop the sensors searching for the highest power in the cluster for sending the information.

Reference Reference Referencias

1. Adnan, L.H., Yussoff, Y.M. & Hashim, H. 2010,'Secure Boot Process for Wireless Sensor Node', International Conference on Computer Applications and Industrial Electronics (ICCAIE), pp. 646- 649.
2. Boukerch, A., Xu, L. & El-khatib, K. 2007,'Trusted-based security for wireless as hoc and sensor networks', computer communications, vol. 30, pp. 2413-2427.
3. Bashir, A. & Mir, A.S. 2013,'An Energy Efficient and Dynamic Security Protocol for Wireless Sensor Network', International Conference on Advance Electronic System (ICAES), pp. 257-261.
4. Badakhshan, M. & Arifler, D. 2007,'Simulation Based Analysis of Spreading Dynamic of Malware in Wireless Sensor Network', International Conference on Sensor Technologies and Applications, vol. 65, pp. 164-169.

5. Dargi, W. & Poellabauer, C. 2010, Fundamentals of Wireless Sensor Networks, 1st edn, Wiley Series on Wireless Communications and Mobile Computing, John Wiley & Sons Ltd, Chichester, UK.
6. Fessant, F.L., Papadimitriou, A., Viana, A.C., Sengul, C. & Palomar, E. 2012,'A sinkhole resilient protocol for wireless sensor networks: Performance and security analysis', Computer Communications, vol. 35, pp. 234-248.
7. Haghighi, M.S., Mohamedpour, K., Varadharajan, V. Quinn, B.G. 2011,'Stochastic Modeling of Hello Flooding in Slotted CSMA/CA Wireless Sensor Networks', Transaction on Information Forensics and Security, vol. 6, no. 4, pp. 1185-1199.
8. Hamedheidari, S. & Rafeh, R. 2013,'A novel agent-based approach to detect sinkhole attacks in wireless sensor network', Computer & Security, vol. 37, pp. 1-14.
9. Sreelaja, N.K. & Pai, G.A.V. 2014,'Swarm intelligence based approach for sinkhole attack detection in wireless sensor networks', Applied Soft Computing, vol. 19, pp. 68- 79.
10. Karlof, C. & Wagner, D. 2003,'Secure routing in wireless sensor network: attacks and countermeasures', Ad Hoc Networks, vol. 1, pp. 293-315.
11. Magotra, S. & Kumar, K. 2014,'Detection of HELLO flood attack on LEACH protocol', International Advance Computing Conference (IACC), pp. 193-198.
12. Pathan, A.K., Lee, H & Hong, C.S. 2006,'Security in Wireless Sensor Network: Issues and Challengies', ISBN, pp. 1043-1048.
13. Sarma, H.K.D & Kar, A. 2006,'Security Threats in Wireless Sensor Networks', IEEE, pp. 243-251.
14. Sarma, H.K.D & Kar, A. 2008,'Security Threats in Wireless Sensor Networks', IEE A&E System Magazine, Jun, pp. 39- 45.
15. Shafiei, H., Khonsari, A., Derakhshi, H. & Mousavi, P. 2014,'Detection and mitigation of sinkhole attacks in wireless sensor network', Journal of Computer and System Science, vol. 80, pp. 644-653.
16. Stafrace, S.K. & Antonopoulos, N. 2010,'Malitary tactics in agent-based sinkhole attack detection for wireless ad hoc networks', computer Communications, vol. 33, pp. 619-638.
17. Tahir, H. & Shah, S.A.A. 2008,'Wireless Sensor Networks-A Security Prespective', IEEE, pp. 189-193.
18. Wang, Y., Lin, W. & Zhang, T. 2010,'Study on Security of Wireless Sensor Networks in Smart Grid', International Conference on Power Technology, pp. 1-7.
19. Zhang, X., He, J. & Wei, Q. 2009,'Security Considerations on Node Mobility in Wireless Sensor Networks', Fourth International Conference on Computer Science and Convergence Information Technology, vol. 275, pp. 1143-1146.
20. Zhang, F., Zhai, L., Yang, J. & Cui, X. 2014,'Sinkhole attack detection based on redundancy mechanism in wireless sensor network', Information Technology in Quantitative Management (ITQM), vol. 31, pp. 711-720.

Global Journals Inc. (US) Guidelines Handbook 2015

www.GlobalJournals.org

FELLOW OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (FARSC)

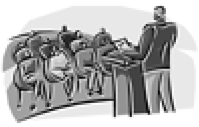
Global Journals Incorporate (USA) is accredited by Open Association of Research Society (OARS), U.S.A and in turn, awards "FARSC" title to individuals. The 'FARSC' title is accorded to a selected professional after the approval of the Editor-in-Chief/Editorial Board Members/Dean.

- The "FARSC" is a dignified title which is accorded to a person's name viz. Dr. John E. Hall, Ph.D., FARSC or William Walldroff, M.S., FARSC.

FARSC accrediting is an honor. It authenticates your research activities. After recognition as FARSC, you can add 'FARSC' title with your name as you use this recognition as additional suffix to your status. This will definitely enhance and add more value and repute to your name. You may use it on your professional Counseling Materials such as CV, Resume, and Visiting Card etc.

The following benefits can be availed by you only for next three years from the date of certification:

FARSC designated members are entitled to avail a 40% discount while publishing their research papers (of a single author) with Global Journals Incorporation (USA), if the same is accepted by Editorial Board/Peer Reviewers. If you are a main author or co-author in case of multiple authors, you will be entitled to avail discount of 10%.



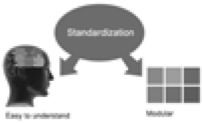
Once FARSC title is accorded, the Fellow is authorized to organize a symposium/seminar/conference on behalf of Global Journal Incorporation (USA).The Fellow can also participate in conference/seminar/symposium organized by another institution as representative of Global Journal. In both the cases, it is mandatory for him to discuss with us and obtain our consent.

You may join as member of the Editorial Board of Global Journals Incorporation (USA) after successful completion of three years as Fellow and as Peer Reviewer. In addition, it is also desirable that you should organize seminar/symposium/conference at least once.

We shall provide you intimation regarding launching of e-version of journal of your stream time to time. This may be utilized in your library for the enrichment of knowledge of your students as well as it can also be helpful for the concerned faculty members.

The FARSC can go through standards of OARS. You can also play vital role if you have any suggestions so that proper amendment can take place to improve the same for the benefit of entire research community.

As FARSC, you will be given a renowned, secure and free professional email address with 100 GB of space e.g. johnhall@globaljournals.org. This will include Webmail, Spam Assassin, Email Forwarders, Auto-Responders, Email Delivery Route tracing, etc.



The FARSC will be eligible for a free application of standardization of their researches. Standardization of research will be subject to acceptability within stipulated norms as the next step after publishing in a journal. We shall depute a team of specialized research professionals who will render their services for elevating your researches to next higher level, which is worldwide open standardization.

The FARSC member can apply for grading and certification of standards of their educational and Institutional Degrees to Open Association of Research, Society U.S.A. Once you are designated as FARSC, you may send us a scanned copy of all of your credentials. OARS will verify, grade and certify them. This will be based on your academic records, quality of research papers published by you, and some more criteria. After certification of all your credentials by OARS, they will be published on your Fellow Profile link on website https://associationofresearch.org which will be helpful to upgrade the dignity.

The FARSC members can avail the benefits of free research podcasting in Global Research Radio with their research documents. After publishing the work, (including published elsewhere worldwide with proper authorization) you can upload your research paper with your recorded voice or you can utilize chargeable services of our professional RJs to record your paper in their voice on request.

The FARSC member also entitled to get the benefits of free research podcasting of their research documents through video clips. We can also streamline your conference videos and display your slides/ online slides and online research video clips at reasonable charges, on request.

The FARSC is eligible to earn from sales proceeds of his/her researches/reference/review Books or literature, while publishing with Global Journals. The FARSC can decide whether he/she would like to publish his/her research in a closed manner. In this case, whenever readers purchase that individual research paper for reading, maximum 60% of its profit earned as royalty by Global Journals, will be credited to his/her bank account. The entire entitled amount will be credited to his/her bank account exceeding limit of minimum fixed balance. There is no minimum time limit for collection. The FARSC member can decide its price and we can help in making the right decision.

The FARSC member is eligible to join as a paid peer reviewer at Global Journals Incorporation (USA) and can get remuneration of 15% of author fees, taken from the author of a respective paper. After reviewing 5 or more papers you can request to transfer the amount to your bank account.

MEMBER OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (MARSC)

The ' MARSC ' title is accorded to a selected professional after the approval of the Editor-in-Chief / Editorial Board Members/Dean.
The “MARSC” is a dignified ornament which is accorded to a person’s name viz. Dr. John E. Hall, Ph.D., MARSC or William Walldroff, M.S., MARSC.

MARSC accrediting is an honor. It authenticates your research activities. After becoming MARSC, you can add 'MARSC' title with your name as you use this recognition as additional suffix to your status. This will definitely enhance and add more value and repute to your name. You may use it on your professional Counseling Materials such as CV, Resume, Visiting Card and Name Plate etc.

The following benefitscan be availed by you only for next three years from the date of certification.

MARSC designated members are entitled to avail a 25% discount while publishing their research papers (of a single author) in Global Journals Inc., if the same is accepted by our Editorial Board and Peer Reviewers. If you are a main author or co-author of a group of authors, you will get discount of 10%.

As MARSC, you will be given a renowned, secure and free professional email address with 30 GB of space e.g. johnhall@globaljournals.org. This will include Webmail, Spam Assassin, Email Forwarders, Auto-Responders, Email Delivery Route tracing, etc.

We shall provide you intimation regarding launching of e-version of journal of your stream time to time. This may be utilized in your library for the enrichment of knowledge of your students as well as it can also be helpful for the concerned faculty members.

The MARSC member can apply for approval, grading and certification of standards of their educational and Institutional Degrees to Open Association of Research, Society U.S.A.

Once you are designated as MARSC, you may send us a scanned copy of all of your credentials. OARS will verify, grade and certify them. This will be based on your academic records, quality of research papers published by you, and some more criteria.

It is mandatory to read all terms and conditions carefully.

Auxiliary Memberships

Institutional Fellow of Open Association of Research Society (USA)-OARS (USA)

Global Journals Incorporation (USA) is accredited by Open Association of Research Society, U.S.A (OARS) and in turn, affiliates research institutions as “Institutional Fellow of Open Association of Research Society” (IFOARS).

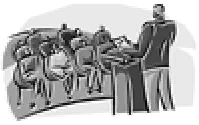
The “FARSC” is a dignified title which is accorded to a person’s name viz. Dr. John E. Hall, Ph.D., FARSC or William Walldroff, M.S., FARSC.

The IFOARS institution is entitled to form a Board comprised of one Chairperson and three to five board members preferably from different streams. The Board will be recognized as “Institutional Board of Open Association of Research Society”-(IBOARS).

The Institute will be entitled to following benefits:

The IBOARS can initially review research papers of their institute and recommend them to publish with respective journal of Global Journals. It can also review the papers of other institutions after obtaining our consent. The second review will be done by peer reviewer of Global Journals Incorporation (USA) The Board is at liberty to appoint a peer reviewer with the approval of chairperson after consulting us.

The author fees of such paper may be waived off up to 40%.



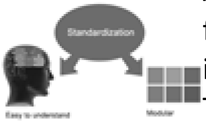
The Global Journals Incorporation (USA) at its discretion can also refer double blind peer reviewed paper at their end to the board for the verification and to get recommendation for final stage of acceptance of publication.

The IBOARS can organize symposium/seminar/conference in their country on behalf of Global Journals Incorporation (USA)-OARS (USA). The terms and conditions can be discussed separately.

The Board can also play vital role by exploring and giving valuable suggestions regarding the Standards of “Open Association of Research Society, U.S.A (OARS)” so that proper amendment can take place for the benefit of entire research community. We shall provide details of particular standard only on receipt of request from the Board.

The board members can also join us as Individual Fellow with 40% discount on total fees applicable to Individual Fellow. They will be entitled to avail all the benefits as declared. Please visit Individual Fellow-sub menu of GlobalJournals.org to have more relevant details.

We shall provide you intimation regarding launching of e-version of journal of your stream time to time. This may be utilized in your library for the enrichment of knowledge of your students as well as it can also be helpful for the concerned faculty members.



After nomination of your institution as "Institutional Fellow" and constantly functioning successfully for one year, we can consider giving recognition to your institute to function as Regional/Zonal office on our behalf.
The board can also take up the additional allied activities for betterment after our consultation.

The following entitlements are applicable to individual Fellows:

Open Association of Research Society, U.S.A (OARS) By-laws states that an individual Fellow may use the designations as applicable, or the corresponding initials. The Credentials of individual Fellow and Associate designations signify that the individual has gained knowledge of the fundamental concepts. One is magnanimous and proficient in an expertise course covering the professional code of conduct, and follows recognized standards of practice.

Open Association of Research Society (US)/ Global Journals Incorporation (USA), as described in Corporate Statements, are educational, research publishing and professional membership organizations. Achieving our individual Fellow or Associate status is based mainly on meeting stated educational research requirements.

Disbursement of 40% Royalty earned through Global Journals : Researcher = 50%, Peer Reviewer = 37.50%, Institution = 12.50% E.g. Out of 40%, the 20% benefit should be passed on to researcher, 15 % benefit towards remuneration should be given to a reviewer and remaining 5% is to be retained by the institution.

We shall provide print version of 12 issues of any three journals [as per your requirement] out of our 38 journals worth $ 2376 USD.

Other:

The individual Fellow and Associate designations accredited by Open Association of Research Society (US) credentials signify guarantees following achievements:

- The professional accredited with Fellow honor, is entitled to various benefits viz. name, fame, honor, regular flow of income, secured bright future, social status etc.

- In addition to above, if one is single author, then entitled to 40% discount on publishing research paper and can get 10%discount if one is co-author or main author among group of authors.
- The Fellow can organize symposium/seminar/conference on behalf of Global Journals Incorporation (USA) and he/she can also attend the same organized by other institutes on behalf of Global Journals.
- The Fellow can become member of Editorial Board Member after completing 3yrs.
- The Fellow can earn 60% of sales proceeds from the sale of reference/review books/literature/publishing of research paper.
- Fellow can also join as paid peer reviewer and earn 15% remuneration of author charges and can also get an opportunity to join as member of the Editorial Board of Global Journals Incorporation (USA)
- • This individual has learned the basic methods of applying those concepts and techniques to common challenging situations. This individual has further demonstrated an in–depth understanding of the application of suitable techniques to a particular area of research practice.

Note :

> "
>
> - In future, if the board feels the necessity to change any board member, the same can be done with the consent of the chairperson along with anyone board member without our approval.
> - In case, the chairperson needs to be replaced then consent of 2/3rd board members are required and they are also required to jointly pass the resolution copy of which should be sent to us. In such case, it will be compulsory to obtain our approval before replacement.
> - In case of "Difference of Opinion [if any]" among the Board members, our decision will be final and binding to everyone.
>
> "

Process of submission of Research Paper

The Area or field of specialization may or may not be of any category as mentioned in 'Scope of Journal' menu of the GlobalJournals.org website. There are 37 Research Journal categorized with Six parental Journals GJCST, GJMR, GJRE, GJMBR, GJSFR, GJHSS. For Authors should prefer the mentioned categories. There are three widely used systems UDC, DDC and LCC. The details are available as 'Knowledge Abstract' at Home page. The major advantage of this coding is that, the research work will be exposed to and shared with all over the world as we are being abstracted and indexed worldwide.

The paper should be in proper format. The format can be downloaded from first page of 'Author Guideline' Menu. The Author is expected to follow the general rules as mentioned in this menu. The paper should be written in MS-Word Format (*.DOC,*.DOCX).

The Author can submit the paper either online or offline. The authors should prefer online submission.Online Submission: There are three ways to submit your paper:

(A) (I) First, register yourself using top right corner of Home page then Login. If you are already registered, then login using your username and password.

(II) Choose corresponding Journal.

(III) Click 'Submit Manuscript'. Fill required information and Upload the paper.

(B) If you are using Internet Explorer, then Direct Submission through Homepage is also available.

(C) If these two are not convenient, and then email the paper directly to dean@globaljournals.org.

Offline Submission: Author can send the typed form of paper by Post. However, online submission should be preferred.

Preferred Author Guidelines

MANUSCRIPT STYLE INSTRUCTION (Must be strictly followed)

Page Size: 8.27" X 11'"

- Left Margin: 0.65
- Right Margin: 0.65
- Top Margin: 0.75
- Bottom Margin: 0.75
- Font type of all text should be Swis 721 Lt BT.
- Paper Title should be of Font Size 24 with one Column section.
- Author Name in Font Size of 11 with one column as of Title.
- Abstract Font size of 9 Bold, "Abstract" word in Italic Bold.
- Main Text: Font size 10 with justified two columns section
- Two Column with Equal Column with of 3.38 and Gaping of .2
- First Character must be three lines Drop capped.
- Paragraph before Spacing of 1 pt and After of 0 pt.
- Line Spacing of 1 pt
- Large Images must be in One Column
- Numbering of First Main Headings (Heading 1) must be in Roman Letters, Capital Letter, and Font Size of 10.
- Numbering of Second Main Headings (Heading 2) must be in Alphabets, Italic, and Font Size of 10.

You can use your own standard format also.
Author Guidelines:

1. General,

2. Ethical Guidelines,

3. Submission of Manuscripts,

4. Manuscript's Category,

5. Structure and Format of Manuscript,

6. After Acceptance.

1. GENERAL

Before submitting your research paper, one is advised to go through the details as mentioned in following heads. It will be beneficial, while peer reviewer justify your paper for publication.

Scope

The Global Journals Inc. (US) welcome the submission of original paper, review paper, survey article relevant to the all the streams of Philosophy and knowledge. The Global Journals Inc. (US) is parental platform for Global Journal of Computer Science and Technology, Researches in Engineering, Medical Research, Science Frontier Research, Human Social Science, Management, and Business organization. The choice of specific field can be done otherwise as following in Abstracting and Indexing Page on this Website. As the all Global

Journals Inc. (US) are being abstracted and indexed (in process) by most of the reputed organizations. Topics of only narrow interest will not be accepted unless they have wider potential or consequences.

2. ETHICAL GUIDELINES

Authors should follow the ethical guidelines as mentioned below for publication of research paper and research activities.

Papers are accepted on strict understanding that the material in whole or in part has not been, nor is being, considered for publication elsewhere. If the paper once accepted by Global Journals Inc. (US) and Editorial Board, will become the copyright of the Global Journals Inc. (US).

Authorship: The authors and coauthors should have active contribution to conception design, analysis and interpretation of findings. They should critically review the contents and drafting of the paper. All should approve the final version of the paper before submission

The Global Journals Inc. (US) follows the definition of authorship set up by the Global Academy of Research and Development. According to the Global Academy of R&D authorship, criteria must be based on:

1) Substantial contributions to conception and acquisition of data, analysis and interpretation of the findings.

2) Drafting the paper and revising it critically regarding important academic content.

3) Final approval of the version of the paper to be published.

All authors should have been credited according to their appropriate contribution in research activity and preparing paper. Contributors who do not match the criteria as authors may be mentioned under Acknowledgement.

Acknowledgements: Contributors to the research other than authors credited should be mentioned under acknowledgement. The specifications of the source of funding for the research if appropriate can be included. Suppliers of resources may be mentioned along with address.

Appeal of Decision: The Editorial Board's decision on publication of the paper is final and cannot be appealed elsewhere.

Permissions: It is the author's responsibility to have prior permission if all or parts of earlier published illustrations are used in this paper.

Please mention proper reference and appropriate acknowledgements wherever expected.

If all or parts of previously published illustrations are used, permission must be taken from the copyright holder concerned. It is the author's responsibility to take these in writing.

Approval for reproduction/modification of any information (including figures and tables) published elsewhere must be obtained by the authors/copyright holders before submission of the manuscript. Contributors (Authors) are responsible for any copyright fee involved.

3. SUBMISSION OF MANUSCRIPTS

Manuscripts should be uploaded via this online submission page. The online submission is most efficient method for submission of papers, as it enables rapid distribution of manuscripts and consequently speeds up the review procedure. It also enables authors to know the status of their own manuscripts by emailing us. Complete instructions for submitting a paper is available below.

Manuscript submission is a systematic procedure and little preparation is required beyond having all parts of your manuscript in a given format and a computer with an Internet connection and a Web browser. Full help and instructions are provided on-screen. As an author, you will be prompted for login and manuscript details as Field of Paper and then to upload your manuscript file(s) according to the instructions.

To avoid postal delays, all transaction is preferred by e-mail. A finished manuscript submission is confirmed by e-mail immediately and your paper enters the editorial process with no postal delays. When a conclusion is made about the publication of your paper by our Editorial Board, revisions can be submitted online with the same procedure, with an occasion to view and respond to all comments.

Complete support for both authors and co-author is provided.

4. MANUSCRIPT'S CATEGORY

Based on potential and nature, the manuscript can be categorized under the following heads:

Original research paper: Such papers are reports of high-level significant original research work.

Review papers: These are concise, significant but helpful and decisive topics for young researchers.

Research articles: These are handled with small investigation and applications.

Research letters: The letters are small and concise comments on previously published matters.

5. STRUCTURE AND FORMAT OF MANUSCRIPT

The recommended size of original research paper is less than seven thousand words, review papers fewer than seven thousands words also.Preparation of research paper or how to write research paper, are major hurdle, while writing manuscript. The research articles and research letters should be fewer than three thousand words, the structure original research paper; sometime review paper should be as follows:

Papers: These are reports of significant research (typically less than 7000 words equivalent, including tables, figures, references), and comprise:

(a)Title should be relevant and commensurate with the theme of the paper.

(b) A brief Summary, “Abstract” (less than 150 words) containing the major results and conclusions.

(c) Up to ten keywords, that precisely identifies the paper's subject, purpose, and focus.

(d) An Introduction, giving necessary background excluding subheadings; objectives must be clearly declared.

(e) Resources and techniques with sufficient complete experimental details (wherever possible by reference) to permit repetition; sources of information must be given and numerical methods must be specified by reference, unless non-standard.

(f) Results should be presented concisely, by well-designed tables and/or figures; the same data may not be used in both; suitable statistical data should be given. All data must be obtained with attention to numerical detail in the planning stage. As reproduced design has been recognized to be important to experiments for a considerable time, the Editor has decided that any paper that appears not to have adequate numerical treatments of the data will be returned un-refereed;

(g) Discussion should cover the implications and consequences, not just recapitulating the results; conclusions should be summarizing.

(h) Brief Acknowledgements.

(i) References in the proper form.

Authors should very cautiously consider the preparation of papers to ensure that they communicate efficiently. Papers are much more likely to be accepted, if they are cautiously designed and laid out, contain few or no errors, are summarizing, and be conventional to the approach and instructions. They will in addition, be published with much less delays than those that require much technical and editorial correction.

The Editorial Board reserves the right to make literary corrections and to make suggestions to improve briefness.

It is vital, that authors take care in submitting a manuscript that is written in simple language and adheres to published guidelines.

Format

Language: The language of publication is UK English. Authors, for whom English is a second language, must have their manuscript efficiently edited by an English-speaking person before submission to make sure that, the English is of high excellence. It is preferable, that manuscripts should be professionally edited.

Standard Usage, Abbreviations, and Units: Spelling and hyphenation should be conventional to The Concise Oxford English Dictionary. Statistics and measurements should at all times be given in figures, e.g. 16 min, except for when the number begins a sentence. When the number does not refer to a unit of measurement it should be spelt in full unless, it is 160 or greater.

Abbreviations supposed to be used carefully. The abbreviated name or expression is supposed to be cited in full at first usage, followed by the conventional abbreviation in parentheses.

Metric SI units are supposed to generally be used excluding where they conflict with current practice or are confusing. For illustration, 1.4 l rather than 1.4 × 10-3 m3, or 4 mm somewhat than 4 × 10-3 m. Chemical formula and solutions must identify the form used, e.g. anhydrous or hydrated, and the concentration must be in clearly defined units. Common species names should be followed by underlines at the first mention. For following use the generic name should be constricted to a single letter, if it is clear.

Structure

All manuscripts submitted to Global Journals Inc. (US), ought to include:

Title: The title page must carry an instructive title that reflects the content, a running title (less than 45 characters together with spaces), names of the authors and co-authors, and the place(s) wherever the work was carried out. The full postal address in addition with the e-mail address of related author must be given. Up to eleven keywords or very brief phrases have to be given to help data retrieval, mining and indexing.

Abstract, used in Original Papers and Reviews:

Optimizing Abstract for Search Engines

Many researchers searching for information online will use search engines such as Google, Yahoo or similar. By optimizing your paper for search engines, you will amplify the chance of someone finding it. This in turn will make it more likely to be viewed and/or cited in a further work. Global Journals Inc. (US) have compiled these guidelines to facilitate you to maximize the web-friendliness of the most public part of your paper.

Key Words

A major linchpin in research work for the writing research paper is the keyword search, which one will employ to find both library and Internet resources.

One must be persistent and creative in using keywords. An effective keyword search requires a strategy and planning a list of possible keywords and phrases to try.

Search engines for most searches, use Boolean searching, which is somewhat different from Internet searches. The Boolean search uses "operators," words (and, or, not, and near) that enable you to expand or narrow your affords. Tips for research paper while preparing research paper are very helpful guideline of research paper.

Choice of key words is first tool of tips to write research paper. Research paper writing is an art.A few tips for deciding as strategically as possible about keyword search:

- One should start brainstorming lists of possible keywords before even begin searching. Think about the most important concepts related to research work. Ask, "What words would a source have to include to be truly valuable in research paper?" Then consider synonyms for the important words.
- It may take the discovery of only one relevant paper to let steer in the right keyword direction because in most databases, the keywords under which a research paper is abstracted are listed with the paper.
- One should avoid outdated words.

Keywords are the key that opens a door to research work sources. Keyword searching is an art in which researcher's skills are bound to improve with experience and time.

Numerical Methods: Numerical methods used should be clear and, where appropriate, supported by references.

Acknowledgements: Please make these as concise as possible.

References

References follow the Harvard scheme of referencing. References in the text should cite the authors' names followed by the time of their publication, unless there are three or more authors when simply the first author's name is quoted followed by et al. unpublished work has to only be cited where necessary, and only in the text. Copies of references in press in other journals have to be supplied with submitted typescripts. It is necessary that all citations and references be carefully checked before submission, as mistakes or omissions will cause delays.

References to information on the World Wide Web can be given, but only if the information is available without charge to readers on an official site. Wikipedia and Similar websites are not allowed where anyone can change the information. Authors will be asked to make available electronic copies of the cited information for inclusion on the Global Journals Inc. (US) homepage at the judgment of the Editorial Board.

The Editorial Board and Global Journals Inc. (US) recommend that, citation of online-published papers and other material should be done via a DOI (digital object identifier). If an author cites anything, which does not have a DOI, they run the risk of the cited material not being noticeable.

The Editorial Board and Global Journals Inc. (US) recommend the use of a tool such as Reference Manager for reference management and formatting.

Tables, Figures and Figure Legends

Tables: Tables should be few in number, cautiously designed, uncrowned, and include only essential data. Each must have an Arabic number, e.g. Table 4, a self-explanatory caption and be on a separate sheet. Vertical lines should not be used.

Figures: Figures are supposed to be submitted as separate files. Always take in a citation in the text for each figure using Arabic numbers, e.g. Fig. 4. Artwork must be submitted online in electronic form by e-mailing them.

Preparation of Electronic Figures for Publication

Even though low quality images are sufficient for review purposes, print publication requires high quality images to prevent the final product being blurred or fuzzy. Submit (or e-mail) EPS (line art) or TIFF (halftone/photographs) files only. MS PowerPoint and Word Graphics are unsuitable for printed pictures. Do not use pixel-oriented software. Scans (TIFF only) should have a resolution of at least 350 dpi (halftone) or 700 to 1100 dpi (line drawings) in relation to the imitation size. Please give the data for figures in black and white or submit a Color Work Agreement Form. EPS files must be saved with fonts embedded (and with a TIFF preview, if possible).

For scanned images, the scanning resolution (at final image size) ought to be as follows to ensure good reproduction: line art: >650 dpi; halftones (including gel photographs) : >350 dpi; figures containing both halftone and line images: >650 dpi.

Color Charges: It is the rule of the Global Journals Inc. (US) for authors to pay the full cost for the reproduction of their color artwork. Hence, please note that, if there is color artwork in your manuscript when it is accepted for publication, we would require you to complete and return a color work agreement form before your paper can be published.

Figure Legends: Self-explanatory legends of all figures should be incorporated separately under the heading 'Legends to Figures'. In the full-text online edition of the journal, figure legends may possibly be truncated in abbreviated links to the full screen version. Therefore, the first 100 characters of any legend should notify the reader, about the key aspects of the figure.

6. AFTER ACCEPTANCE

Upon approval of a paper for publication, the manuscript will be forwarded to the dean, who is responsible for the publication of the Global Journals Inc. (US).

6.1 Proof Corrections

The corresponding author will receive an e-mail alert containing a link to a website or will be attached. A working e-mail address must therefore be provided for the related author.

Acrobat Reader will be required in order to read this file. This software can be downloaded

(Free of charge) from the following website:

www.adobe.com/products/acrobat/readstep2.html. This will facilitate the file to be opened, read on screen, and printed out in order for any corrections to be added. Further instructions will be sent with the proof.

Proofs must be returned to the dean at dean@globaljournals.org within three days of receipt.

As changes to proofs are costly, we inquire that you only correct typesetting errors. All illustrations are retained by the publisher. Please note that the authors are responsible for all statements made in their work, including changes made by the copy editor.

6.2 Early View of Global Journals Inc. (US) (Publication Prior to Print)

The Global Journals Inc. (US) are enclosed by our publishing's Early View service. Early View articles are complete full-text articles sent in advance of their publication. Early View articles are absolute and final. They have been completely reviewed, revised and edited for publication, and the authors' final corrections have been incorporated. Because they are in final form, no changes can be made after sending them. The nature of Early View articles means that they do not yet have volume, issue or page numbers, so Early View articles cannot be cited in the conventional way.

6.3 Author Services

Online production tracking is available for your article through Author Services. Author Services enables authors to track their article - once it has been accepted - through the production process to publication online and in print. Authors can check the status of their articles online and choose to receive automated e-mails at key stages of production. The authors will receive an e-mail with a unique link that enables them to register and have their article automatically added to the system. Please ensure that a complete e-mail address is provided when submitting the manuscript.

6.4 Author Material Archive Policy

Please note that if not specifically requested, publisher will dispose off hardcopy & electronic information submitted, after the two months of publication. If you require the return of any information submitted, please inform the Editorial Board or dean as soon as possible.

6.5 Offprint and Extra Copies

A PDF offprint of the online-published article will be provided free of charge to the related author, and may be distributed according to the Publisher's terms and conditions. Additional paper offprint may be ordered by emailing us at: editor@globaljournals.org .

You must strictly follow above Author Guidelines before submitting your paper or else we will not at all be responsible for any corrections in future in any of the way.

Before start writing a good quality Computer Science Research Paper, let us first understand what is Computer Science Research Paper? So, Computer Science Research Paper is the paper which is written by professionals or scientists who are associated to Computer Science and Information Technology, or doing research study in these areas. If you are novel to this field then you can consult about this field from your supervisor or guide.

TECHNIQUES FOR WRITING A GOOD QUALITY RESEARCH PAPER:

1. Choosing the topic: In most cases, the topic is searched by the interest of author but it can be also suggested by the guides. You can have several topics and then you can judge that in which topic or subject you are finding yourself most comfortable. This can be done by asking several questions to yourself, like Will I be able to carry our search in this area? Will I find all necessary recourses to accomplish the search? Will I be able to find all information in this field area? If the answer of these types of questions will be "Yes" then you can choose that topic. In most of the cases, you may have to conduct the surveys and have to visit several places because this field is related to Computer Science and Information Technology. Also, you may have to do a lot of work to find all rise and falls regarding the various data of that subject. Sometimes, detailed information plays a vital role, instead of short information.

2. Evaluators are human: First thing to remember that evaluators are also human being. They are not only meant for rejecting a paper. They are here to evaluate your paper. So, present your Best.

3. Think Like Evaluators: If you are in a confusion or getting demotivated that your paper will be accepted by evaluators or not, then think and try to evaluate your paper like an Evaluator. Try to understand that what an evaluator wants in your research paper and automatically you will have your answer.

4. Make blueprints of paper: The outline is the plan or framework that will help you to arrange your thoughts. It will make your paper logical. But remember that all points of your outline must be related to the topic you have chosen.

5. Ask your Guides: If you are having any difficulty in your research, then do not hesitate to share your difficulty to your guide (if you have any). They will surely help you out and resolve your doubts. If you can't clarify what exactly you require for your work then ask the supervisor to help you with the alternative. He might also provide you the list of essential readings.

6. Use of computer is recommended: As you are doing research in the field of Computer Science, then this point is quite obvious.

7. Use right software: Always use good quality software packages. If you are not capable to judge good software then you can lose quality of your paper unknowingly. There are various software programs available to help you, which you can get through Internet.

8. Use the Internet for help: An excellent start for your paper can be by using the Google. It is an excellent search engine, where you can have your doubts resolved. You may also read some answers for the frequent question how to write my research paper or find model research paper. From the internet library you can download books. If you have all required books make important reading selecting and analyzing the specified information. Then put together research paper sketch out.

9. Use and get big pictures: Always use encyclopedias, Wikipedia to get pictures so that you can go into the depth.

10. Bookmarks are useful: When you read any book or magazine, you generally use bookmarks, right! It is a good habit, which helps to not to lose your continuity. You should always use bookmarks while searching on Internet also, which will make your search easier.

11. Revise what you wrote: When you write anything, always read it, summarize it and then finalize it.

12. Make all efforts: Make all efforts to mention what you are going to write in your paper. That means always have a good start. Try to mention everything in introduction, that what is the need of a particular research paper. Polish your work by good skill of writing and always give an evaluator, what he wants.

13. Have backups: When you are going to do any important thing like making research paper, you should always have backup copies of it either in your computer or in paper. This will help you to not to lose any of your important.

14. Produce good diagrams of your own: Always try to include good charts or diagrams in your paper to improve quality. Using several and unnecessary diagrams will degrade the quality of your paper by creating "hotchpotch." So always, try to make and include those diagrams, which are made by your own to improve readability and understandability of your paper.

15. Use of direct quotes: When you do research relevant to literature, history or current affairs then use of quotes become essential but if study is relevant to science then use of quotes is not preferable.

16. Use proper verb tense: Use proper verb tenses in your paper. Use past tense, to present those events that happened. Use present tense to indicate events that are going on. Use future tense to indicate future happening events. Use of improper and wrong tenses will confuse the evaluator. Avoid the sentences that are incomplete.

17. Never use online paper: If you are getting any paper on Internet, then never use it as your research paper because it might be possible that evaluator has already seen it or maybe it is outdated version.

18. Pick a good study spot: To do your research studies always try to pick a spot, which is quiet. Every spot is not for studies. Spot that suits you choose it and proceed further.

19. Know what you know: Always try to know, what you know by making objectives. Else, you will be confused and cannot achieve your target.

20. Use good quality grammar: Always use a good quality grammar and use words that will throw positive impact on evaluator. Use of good quality grammar does not mean to use tough words, that for each word the evaluator has to go through dictionary. Do not start sentence with a conjunction. Do not fragment sentences. Eliminate one-word sentences. Ignore passive voice. Do not ever use a big word when a diminutive one would suffice. Verbs have to be in agreement with their subjects. Prepositions are not expressions to finish sentences with. It is incorrect to ever divide an infinitive. Avoid clichés like the disease. Also, always shun irritating alliteration. Use language that is simple and straight forward. put together a neat summary.

21. Arrangement of information: Each section of the main body should start with an opening sentence and there should be a changeover at the end of the section. Give only valid and powerful arguments to your topic. You may also maintain your arguments with records.

22. Never start in last minute: Always start at right time and give enough time to research work. Leaving everything to the last minute will degrade your paper and spoil your work.

23. Multitasking in research is not good: Doing several things at the same time proves bad habit in case of research activity. Research is an area, where everything has a particular time slot. Divide your research work in parts and do particular part in particular time slot.

24. Never copy others' work: Never copy others' work and give it your name because if evaluator has seen it anywhere you will be in trouble.

25. Take proper rest and food: No matter how many hours you spend for your research activity, if you are not taking care of your health then all your efforts will be in vain. For a quality research, study is must, and this can be done by taking proper rest and food.

26. Go for seminars: Attend seminars if the topic is relevant to your research area. Utilize all your resources.

27. Refresh your mind after intervals: Try to give rest to your mind by listening to soft music or by sleeping in intervals. This will also improve your memory.

28. Make colleagues: Always try to make colleagues. No matter how sharper or intelligent you are, if you make colleagues you can have several ideas, which will be helpful for your research.

29. Think technically: Always think technically. If anything happens, then search its reasons, its benefits, and demerits.

30. Think and then print: When you will go to print your paper, notice that tables are not be split, headings are not detached from their descriptions, and page sequence is maintained.

31. Adding unnecessary information: Do not add unnecessary information, like, I have used MS Excel to draw graph. Do not add irrelevant and inappropriate material. These all will create superfluous. Foreign terminology and phrases are not apropos. One should NEVER take a broad view. Analogy in script is like feathers on a snake. Not at all use a large word when a very small one would be sufficient. Use words properly, regardless of how others use them. Remove quotations. Puns are for kids, not grunt readers. Amplification is a billion times of inferior quality than sarcasm.

32. Never oversimplify everything: To add material in your research paper, never go for oversimplification. This will definitely irritate the evaluator. Be more or less specific. Also too, by no means, ever use rhythmic redundancies. Contractions aren't essential and shouldn't be there used. Comparisons are as terrible as clichés. Give up ampersands and abbreviations, and so on. Remove commas, that are, not necessary. Parenthetical words however should be together with this in commas. Understatement is all the time the complete best way to put onward earth-shaking thoughts. Give a detailed literary review.

33. Report concluded results: Use concluded results. From raw data, filter the results and then conclude your studies based on measurements and observations taken. Significant figures and appropriate number of decimal places should be used. Parenthetical remarks are prohibitive. Proofread carefully at final stage. In the end give outline to your arguments. Spot out perspectives of further study of this subject. Justify your conclusion by at the bottom of them with sufficient justifications and examples.

34. After conclusion: Once you have concluded your research, the next most important step is to present your findings. Presentation is extremely important as it is the definite medium though which your research is going to be in print to the rest of the crowd. Care should be taken to categorize your thoughts well and present them in a logical and neat manner. A good quality research paper format is essential because it serves to highlight your research paper and bring to light all necessary aspects in your research.

Informal Guidelines of Research Paper Writing

Key points to remember:

- Submit all work in its final form.
- Write your paper in the form, which is presented in the guidelines using the template.
- Please note the criterion for grading the final paper by peer-reviewers.

Final Points:

A purpose of organizing a research paper is to let people to interpret your effort selectively. The journal requires the following sections, submitted in the order listed, each section to start on a new page.

The introduction will be compiled from reference matter and will reflect the design processes or outline of basis that direct you to make study. As you will carry out the process of study, the method and process section will be constructed as like that. The result segment will show related statistics in nearly sequential order and will direct the reviewers next to the similar intellectual paths throughout the data that you took to carry out your study. The discussion section will provide understanding of the data and projections as to the implication of the results. The use of good quality references all through the paper will give the effort trustworthiness by representing an alertness of prior workings.

Writing a research paper is not an easy job no matter how trouble-free the actual research or concept. Practice, excellent preparation, and controlled record keeping are the only means to make straightforward the progression.

General style:

Specific editorial column necessities for compliance of a manuscript will always take over from directions in these general guidelines.

To make a paper clear

· Adhere to recommended page limits

Mistakes to evade

- Insertion a title at the foot of a page with the subsequent text on the next page
- Separating a table/chart or figure - impound each figure/table to a single page
- Submitting a manuscript with pages out of sequence

In every sections of your document

· Use standard writing style including articles ("a", "the," etc.)

· Keep on paying attention on the research topic of the paper

· Use paragraphs to split each significant point (excluding for the abstract)

· Align the primary line of each section

· Present your points in sound order

· Use present tense to report well accepted

· Use past tense to describe specific results

· Shun familiar wording, don't address the reviewer directly, and don't use slang, slang language, or superlatives

· Shun use of extra pictures - include only those figures essential to presenting results

Title Page:

Choose a revealing title. It should be short. It should not have non-standard acronyms or abbreviations. It should not exceed two printed lines. It should include the name(s) and address (es) of all authors.

Abstract:

The summary should be two hundred words or less. It should briefly and clearly explain the key findings reported in the manuscript--must have precise statistics. It should not have abnormal acronyms or abbreviations. It should be logical in itself. Shun citing references at this point.

An abstract is a brief distinct paragraph summary of finished work or work in development. In a minute or less a reviewer can be taught the foundation behind the study, common approach to the problem, relevant results, and significant conclusions or new questions.

Write your summary when your paper is completed because how can you write the summary of anything which is not yet written? Wealth of terminology is very essential in abstract. Yet, use comprehensive sentences and do not let go readability for briefness. You can maintain it succinct by phrasing sentences so that they provide more than lone rationale. The author can at this moment go straight to shortening the outcome. Sum up the study, with the subsequent elements in any summary. Try to maintain the initial two items to no more than one ruling each.

- Reason of the study - theory, overall issue, purpose
- Fundamental goal
- To the point depiction of the research
- Consequences, including definite statistics - if the consequences are quantitative in nature, account quantitative data; results of any numerical analysis should be reported
- Significant conclusions or questions that track from the research(es)

Approach:

- Single section, and succinct
- As a outline of job done, it is always written in past tense
- A conceptual should situate on its own, and not submit to any other part of the paper such as a form or table
- Center on shortening results - bound background information to a verdict or two, if completely necessary
- What you account in an conceptual must be regular with what you reported in the manuscript
- Exact spelling, clearness of sentences and phrases, and appropriate reporting of quantities (proper units, important statistics) are just as significant in an abstract as they are anywhere else

Introduction:

The **Introduction** should "introduce" the manuscript. The reviewer should be presented with sufficient background information to be capable to comprehend and calculate the purpose of your study without having to submit to other works. The basis for the study should be offered. Give most important references but shun difficult to make a comprehensive appraisal of the topic. In the introduction, describe the problem visibly. If the problem is not acknowledged in a logical, reasonable way, the reviewer will have no attention in your result. Speak in common terms about techniques used to explain the problem, if needed, but do not present any particulars about the protocols here. Following approach can create a valuable beginning:

- Explain the value (significance) of the study
- Shield the model - why did you employ this particular system or method? What is its compensation? You strength remark on its appropriateness from a abstract point of vision as well as point out sensible reasons for using it.
- Present a justification. Status your particular theory (es) or aim(s), and describe the logic that led you to choose them.
- Very for a short time explain the tentative propose and how it skilled the declared objectives.

Approach:

- Use past tense except for when referring to recognized facts. After all, the manuscript will be submitted after the entire job is done.
- Sort out your thoughts; manufacture one key point with every section. If you make the four points listed above, you will need a least of four paragraphs.

- Present surroundings information only as desirable in order hold up a situation. The reviewer does not desire to read the whole thing you know about a topic.
- Shape the theory/purpose specifically - do not take a broad view.
- As always, give awareness to spelling, simplicity and correctness of sentences and phrases.

Procedures (Methods and Materials):

This part is supposed to be the easiest to carve if you have good skills. A sound written Procedures segment allows a capable scientist to replacement your results. Present precise information about your supplies. The suppliers and clarity of reagents can be helpful bits of information. Present methods in sequential order but linked methodologies can be grouped as a segment. Be concise when relating the protocols. Attempt for the least amount of information that would permit another capable scientist to spare your outcome but be cautious that vital information is integrated. The use of subheadings is suggested and ought to be synchronized with the results section. When a technique is used that has been well described in another object, mention the specific item describing a way but draw the basic principle while stating the situation. The purpose is to text all particular resources and broad procedures, so that another person may use some or all of the methods in one more study or referee the scientific value of your work. It is not to be a step by step report of the whole thing you did, nor is a methods section a set of orders.

Materials:

- Explain materials individually only if the study is so complex that it saves liberty this way.
- Embrace particular materials, and any tools or provisions that are not frequently found in laboratories.
- Do not take in frequently found.
- If use of a definite type of tools.
- Materials may be reported in a part section or else they may be recognized along with your measures.

Methods:

- Report the method (not particulars of each process that engaged the same methodology)
- Describe the method entirely
- To be succinct, present methods under headings dedicated to specific dealings or groups of measures
- Simplify - details how procedures were completed not how they were exclusively performed on a particular day.
- If well known procedures were used, account the procedure by name, possibly with reference, and that's all.

Approach:

- It is embarrassed or not possible to use vigorous voice when documenting methods with no using first person, which would focus the reviewer's interest on the researcher rather than the job. As a result when script up the methods most authors use third person passive voice.
- Use standard style in this and in every other part of the paper - avoid familiar lists, and use full sentences.

What to keep away from

- Resources and methods are not a set of information.
- Skip all descriptive information and surroundings - save it for the argument.
- Leave out information that is immaterial to a third party.

Results:

The principle of a results segment is to present and demonstrate your conclusion. Create this part a entirely objective details of the outcome, and save all understanding for the discussion.

The page length of this segment is set by the sum and types of data to be reported. Carry on to be to the point, by means of statistics and tables, if suitable, to present consequences most efficiently.You must obviously differentiate material that would usually be incorporated in a study editorial from any unprocessed data or additional appendix matter that would not be available. In fact, such matter should not be submitted at all except requested by the instructor.

Content

- Sum up your conclusion in text and demonstrate them, if suitable, with figures and tables.
- In manuscript, explain each of your consequences, point the reader to remarks that are most appropriate.
- Present a background, such as by describing the question that was addressed by creation an exacting study.
- Explain results of control experiments and comprise remarks that are not accessible in a prescribed figure or table, if appropriate.
- Examine your data, then prepare the analyzed (transformed) data in the form of a figure (graph), table, or in manuscript form.

What to stay away from

- Do not discuss or infer your outcome, report surroundings information, or try to explain anything.
- Not at all, take in raw data or intermediate calculations in a research manuscript.
- Do not present the similar data more than once.
- Manuscript should complement any figures or tables, not duplicate the identical information.
- Never confuse figures with tables - there is a difference.

Approach

- As forever, use past tense when you submit to your results, and put the whole thing in a reasonable order.
- Put figures and tables, appropriately numbered, in order at the end of the report
- If you desire, you may place your figures and tables properly within the text of your results part.

Figures and tables

- If you put figures and tables at the end of the details, make certain that they are visibly distinguished from any attach appendix materials, such as raw facts
- Despite of position, each figure must be numbered one after the other and complete with subtitle
- In spite of position, each table must be titled, numbered one after the other and complete with heading
- All figure and table must be adequately complete that it could situate on its own, divide from text

Discussion:

The Discussion is expected the trickiest segment to write and describe. A lot of papers submitted for journal are discarded based on problems with the Discussion. There is no head of state for how long a argument should be. Position your understanding of the outcome visibly to lead the reviewer through your conclusions, and then finish the paper with a summing up of the implication of the study. The purpose here is to offer an understanding of your results and hold up for all of your conclusions, using facts from your research and generally accepted information, if suitable. The implication of result should be visibly described. Infer your data in the conversation in suitable depth. This means that when you clarify an observable fact you must explain mechanisms that may account for the observation. If your results vary from your prospect, make clear why that may have happened. If your results agree, then explain the theory that the proof supported. It is never suitable to just state that the data approved with prospect, and let it drop at that.

- Make a decision if each premise is supported, discarded, or if you cannot make a conclusion with assurance. Do not just dismiss a study or part of a study as "uncertain."
- Research papers are not acknowledged if the work is imperfect. Draw what conclusions you can based upon the results that you have, and take care of the study as a finished work
- You may propose future guidelines, such as how the experiment might be personalized to accomplish a new idea.
- Give details all of your remarks as much as possible, focus on mechanisms.
- Make a decision if the tentative design sufficiently addressed the theory, and whether or not it was correctly restricted.
- Try to present substitute explanations if sensible alternatives be present.
- One research will not counter an overall question, so maintain the large picture in mind, where do you go next? The best studies unlock new avenues of study. What questions remain?
- Recommendations for detailed papers will offer supplementary suggestions.

Approach:

- When you refer to information, differentiate data generated by your own studies from available information
- Submit to work done by specific persons (including you) in past tense.
- Submit to generally acknowledged facts and main beliefs in present tense.

The Administration Rules

Please carefully note down following rules and regulation before submitting your Research Paper to Global Journals Inc. (US):

Segment Draft and Final Research Paper: You have to strictly follow the template of research paper. If it is not done your paper may get rejected.

- The **major constraint** is that you must independently make all content, tables, graphs, and facts that are offered in the paper. You must write each part of the paper wholly on your own. The Peer-reviewers need to identify your own perceptive of the concepts in your own terms. NEVER extract straight from any foundation, and never rephrase someone else's analysis.
- Do not give permission to anyone else to "PROOFREAD" your manuscript.
- Methods to avoid Plagiarism is applied by us on every paper, if found guilty, you will be blacklisted by all of our collaborated research groups, your institution will be informed for this and strict legal actions will be taken immediately.)
- To guard yourself and others from possible illegal use please do not permit anyone right to use to your paper and files.

CRITERION FOR GRADING A RESEARCH PAPER (COMPILATION) BY GLOBAL JOURNALS INC. (US)

Please note that following table is only a Grading of "Paper Compilation" and not on "Performed/Stated Research" whose grading solely depends on Individual Assigned Peer Reviewer and Editorial Board Member. These can be available only on request and after decision of Paper. This report will be the property of Global Journals Inc. (US).

Topics	Grades		
	A-B	**C-D**	**E-F**
Abstract	Clear and concise with appropriate content, Correct format. 200 words or below	Unclear summary and no specific data, Incorrect form Above 200 words	No specific data with ambiguous information Above 250 words
Introduction	Containing all background details with clear goal and appropriate details, flow specification, no grammar and spelling mistake, well organized sentence and paragraph, reference cited	Unclear and confusing data, appropriate format, grammar and spelling errors with unorganized matter	Out of place depth and content, hazy format
Methods and Procedures	Clear and to the point with well arranged paragraph, precision and accuracy of facts and figures, well organized subheads	Difficult to comprehend with embarrassed text, too much explanation but completed	Incorrect and unorganized structure with hazy meaning
Result	Well organized, Clear and specific, Correct units with precision, correct data, well structuring of paragraph, no grammar and spelling mistake	Complete and embarrassed text, difficult to comprehend	Irregular format with wrong facts and figures
Discussion	Well organized, meaningful specification, sound conclusion, logical and concise explanation, highly structured paragraph reference cited	Wordy, unclear conclusion, spurious	Conclusion is not cited, unorganized, difficult to comprehend
References	Complete and correct format, well organized	Beside the point, Incomplete	Wrong format and structuring

INDEX

save our planet

Global Journal of Computer Science and Technology

Visit us on the Web at www.GlobalJournals.org | www.ComputerResearch.org
or email us at helpdesk@globaljournals.org

9 770116 586982 61427>

ISSN 9754350