Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 15 Issue 5 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 Survey in Wireless Ad Hoc Network Security and Secure Energy Optimization Approaches for Routing

By D V Srihari Babu & Dr. P Chandrashekhar Reddy
JNTUH, Hyderabad, India

Abstract- Wireless ad hoc network nodes together establish a network infrastructure without using any access points or base stations for communicates using multi hop schemes. It has significant characteristics like dynamic topologies, constrained in bandwidth and limited resource a high challenge in implementing security with optimized energy resource utilization which is the key aspects while designing modern ad hoc networks architecture. Ad hoc Networks nodes are limited in broadcast range, and also their capabilities of computation and storage are well limited to their energy resources. This limitation of resources in wireless ad hoc creates high challenges in incorporating security mechanism for routing security and privacy maintenance. This paper investigates the various issues and challenges in secure routing and energy optimization during communication in wireless ad hoc network towards security and secure energy utilization improvisation.

Keywords: *wireless ad hoc network, routing, security, energy resource optimization.*

GJCST-E Classification : *C.2.1 C.2.2*

Strictly as per the compliance and regulations of:

A Survey in Wireless Ad Hoc Network Security and Secure Energy Optimization Approaches for Routing

D V Srihari Babu [α] & Dr. P Chandrashekhar Reddy [σ]

Abstract- **Wireless ad hoc network nodes together establish a network infrastructure without using any access points or base stations for communicates using multi hop schemes. It has significant characteristics like dynamic topologies, constrained in bandwidth and limited resource a high challenge in implementing security with optimized energy resource utilization which is the key aspects while designing modern ad hoc networks architecture. Ad hoc Networks nodes are limited in broadcast range, and also their capabilities of computation and storage are well limited to their energy resources. This limitation of resources in wireless ad hoc creates high challenges in incorporating security mechanism for routing security and privacy maintenance. This paper investigates the various issues and challenges in secure routing and energy optimization during communication in wireless ad hoc network towards security and secure energy utilization improvisation.**

Keywords: wireless ad hoc network, routing, security, energy resource optimization.

I. Introduction

Ad hoc networks where all nodes cooperatively maintain network connectivity in multi-hop wireless networks. Networks of this kind useful for disaster relief and emergency needs through a temporary network connectivity which is required to be used in such situation. It enables communication between nodes by forward packets within each other's. Building such ad hoc networks creates many barriers imposed by the environment and significant technical challenge. Ad hoc network suffers due to high mobility and resource constraints in together. The multiple propagations and intervention in wireless transmission effects and provide wireless primarily on the limited primarily to the wireless medium, operating in an ad hoc network routing protocols combined to create significant challenges. Thus, in the field of lightweight equipment should be used. Because they run on battery lifetime and improve the network of battery life as they should be conserving energy resources.

Wireless mobile ad hoc network (MANET) due to its extensive features is widely used in many military and civilian applications. Ad networks collect data on many Military and civilian applications. Ad hoc networks collect data on many wireless applications that are designed for a variety of environments. Based on the assessment of the different categories of data in their intended application. The natures of the applications mentioned above are used by governments, and individuals concerned. However, data used in among are confidentiality, authenticity and availability must be maintained in the integrity of certification.

Security and resources effect sensors in wireless networks due to its very limited resources of wireless networks and other challenges [3][4]. Mobile ad hoc network operate on traditional security networks services due to the limitations of wireless sensor networks and its difficulties to employ traditional security measures. For example, it is inefficient to employ SSL protocol. SSL protocol for wireless sensor networks, inefficient as it requires a high amount of energy [5][6].

This paper provides an in depth investigation in security issues and secure energy optimization approaches in Wireless mobile ad hoc network. It initially discusses the trends and mechanism of mobile ad hoc network communication in Section-2. Security issues and vulnerabilities are being discussed in section-3 and the energy optimization for longer network stability is discussed in Section-3.

II. Wireless Mobile ad hoc Network

A mobile ad hoc network (MANET) is dynamic arbitrary and temporary network topology to manage the wireless mobile nodes with self-configuration. People and vehicles using the first wireless communication infrastructure or the infrastructure of such areas without the need for an extension can internetwork [3].

All the nodes in Mobile ad-hoc network communicate directly to their range nodes which are in their radio range. Direct communication to communicate with each other within the intermediate node (s), while that of the nodes. In both cases, all nodes are involved in communication with the wireless network automatically, so this can be seen as some kind of mobile ad-hoc network.

Mobile ad hoc network are able to communicate directly to all the other titles in the radio range coverage. To communicate with each other in direct communication range, inter-node (s) that do not

Author α : Assoc. Professor, Dept of ECE Kottam karunakara Reddy inst. of Technology, Kurnool Andhra Pradesh, INDIA-518218.
e-mail: srihari2k1@gmail.com
Author σ : Professor, Department of ECE JNTUH, Hyderabad.

use the neighbor information. In both cases, all the nodes will automatically participate in the wireless communication network can be seen as a mobile ad hoc network as a wireless form. It shows the following unique characteristics [4] as follows:

- Wireless links between nodes that are volatile and unpredictable. As well as the mobility of wireless nodes and nodes with limited power supplies, mobile ad-hoc network of wireless communication links between them involved nodes are not stable.
- Topology dynamic behavior is due to the continuous motion of the nodes, the constant changes in the mobile ad-hoc network topology. The other nodes in the network nodes and part-time into constant move out of radio range, and routing information is changing all the time because of the movement of the nodes.
- Statically configured not to the lack of robust security features in the wireless routing protocol is intended for ad-hoc environments. Ad hoc networks are constantly changing the topology of the routing protocol, because statically configured so as to prevent the kind of attacks and potential attacks to try to make use of every pair of adjacent nodes for routing to incorporate the issue for the need.

The above mentioned features are the traditional mobile ad hoc networks. Wired trend indicates malicious behavior suffers more than the network. Therefore, we must focus more attention to utilization of energy security and security issues in mobile ad hoc networks.

III. Limitation in Securing Manet Networks

MANETs are of much more risk than the network attack mechanism should proceed [2][17]. This is due to the following reasons.

a) Lack of Infrastructure

Ad hoc networks, certification authorities, and the line of servers do not apply to any classical solutions based on any infrastructure to operate independently.

b) Inadequate Physical Security

Mobile wireless networks are more vulnerable to physical security threats, fixed wireless networks, more than the average. Theft, spoofing, and DoS attacks should be carefully considered which are likely to increase. Already the most demanding security systems link security threat reduction wireless networks.

c) Limited Power Supply

Due to the temporary movement of network nodes, the node depends on the battery system for their energy supplies. The power supply can be limited because of denial-of-service attacks and selfishness.

d) Frequent Varying Network Topology

Arbitrary nodes are free to move anywhere. Incidentally network topology change and their distance from other nodes may have no limits. As a result of this spontaneous movement, the reaction gradually makes unidirectional links between nodes as well as to give rise to two directional changes in an unpredictable manner [5].

IV. Different Approaches in Manet for Security

Many different suggestions exist in the literature [17][18][19][20] but how to protect the environment of MANET. Many use cases or the environment can be used only for specific solutions, but protocol of bootstrapping the defense should be able to connect to the network, especially in settings where new issues are arise any time and maintain it is a difficult question. In short, this section will be present to establish securities which are already known.

a) Distributed Security Approach

With the fully distributed gateway to access any server nodes or MANETs, completely self-organized security solutions [16] will be used. Each node in a local public key is to manage the repository. Repositories available can be found using a certificate chain to validate a certificate.

The certificate authority using secret sharing method or action can be decentralized. Using this technique makes it possible to distribute several nodes on a common centralized authority. Many nodes distribute a secrete and deals only through cooperation, can the secret reunion. Unfortunately, this method can be a Sybil attack.

b) Location Dependable Security Approach

Taking advantage of the limited mobility or using localized node in a mobile ad hoc network, the security of the communication paths is introduced to the other possibilities. The so-called imprinting of a security in relation to the use of the direct physical contact. This approach is extended by Balfanz et al. [1] and they propose that the public key certificates to the exchange location-limited channel. In some applications, such as ad-hoc communication with a printer and the use of the bootstrap method is very simple security policy. Because of the mobility of the nodes, this approach increases the distribution network within the security association. For self-organized networks this method is exclusively appropriate.

c) Broadcast Solutions

Mobile ad-hoc network is also supported by the existing transmission networks. The distribution networks of the media (audio and video), but also the data for the channels are made. This data is sent over the secure channel, broadcast encryption schemes are

very useful. If the receivers had previously applied to be included in the information packets for transmission encryption to decrypt and access the data. Broadcast encryption also allows you to remove or exclude former recipients from future broadcasts and data can be encrypted using a symmetric encryption key. We also know that a valid key is used in many different keys encrypted with the receivers. Nodes in the network are transmitted in encrypted keys to a key management block, are stored in. The key to decrypt the data nodes and the maintenance of a credible process to extract the block. The transmission encryption in the sense of broadcast it is introduced in [6]. Displayed little change in the policy of this that allows the user to set up groups [11]. Therefore, only a certain number of senders and receivers of messages can be creating as readable.

d) Trust and Reward Procedures

In a wireless network selfish nodes do not support which generally cause the problem for network performance disruption to MANETs. Support and participation are more attractive and a really good way to have been proposed [14]. The node can participate in a lot of debt often, than not presented any packet nodes. The recompense scheme also drives like operations, e.g. links can often present path for packet headers which will be expressed in more interest. Therefore, the network will be increased confidence. These can be used to secure many other protocols and mechanisms for the MANETs.

V. Security Countermeasure Approaches in Manet

To provide secure communication between the nodes to communicate security is a primary concern in MANET. To provide solutions to the problems involved in the security of mobile networks, we should be able to explain to the two most commonly used methods. Prevention of basic network functions in the early stages of their design is not embedded in the network operation which can be easily threatened.

a) Prevention Mechanism

Prevention of discontent from malicious attacks, such a solution is described by initiating active nodes. In the absence of infrastructure it is difficult to provide prevention using the policies of authentication, access control, encryption and digital signature policy, and also by using traditional methods one can provide the first line of defense. Such tokens or smart card PIN, phrases or used in addition to verification of biometrics is available through some security modules.

b) Reactive Mechanism

Identifying malicious activities and taking actions in reactive protocols mechanisms specifies any evidence of malicious that tries to take punitive measures against the reactive approach. MANET intrusion detection system (IDS) is to support schemes such as the use of enforcement mechanisms, etc. These intrusion detection systems are used to detect the manipulation and disorders. Such as Nuglets, confidant, CORE and selfish node behavior to reduce the implementation of cooperation, such as token-based. In this category, they will be able to recognize and react to the threat of such applications is the ability to induce all the protocols.

c) Security Schemes in Ad hoc Networks

In malicious network activity and specific issues related to the environment it is difficult to distinguish between in ad hoc networking. An ad hoc network malicious nodes at random intervals is to enter and leave as soon as the radio transmission range to avoid detection or disrupt network activity may collude with other malicious nodes. Further complicating the detection of malicious nodes behave only occasionally harmful. In order to get a global view of the network topology makes it difficult to dynamically and quickly, which is expected to become obsolete. In order to achieve the security objectives of many security schemes to succeed, even though none of them ad hoc wireless networks, security aspects of the proposed deals

i. *Intrusion Detection*

Intrusion audit data provide evidence Detection System [17] for capturing the attacks. Based on the audit data type used, intrusion Detection System can be classified as a network-based and host-based. Means of network packets through the network hardware interface former usually runs in the second Test monitors and analyzes events and hospitality programs or users [18].Manipulation detection (use patterns of known attacks) and abnormal detection (known attacks deviation flag): intrusion detection systems can be classified as the methods used. Both methods rely on the use of those packets for packets sniffing and analysis [19].

Zhang and Lee [17] described each node in a wireless ad hoc network IDS intrusion detection and personal responsibility by agents involved in the name of the proposed architecture for intrusion detection and response. It can monitor real-time traffic which has no fixed "focus points" Because, audit collection devices is limited by the range of the radio. Anomalies wireless ad hoc network anomaly detection schemes is expected to be localized, incomplete and possibly from the old information is not easily distinguishable. Therefore, the authors [17] of agents based IDS has proposed a new structure in intrusion detection network to improve security, such as encryption, authentication, secure MAC, security, routing and intrusion prevention techniques, complements. Effective, distributed and collaborative construction and preferably it should have been implemented in the detection of an anomaly. If all

the networking layers and incorporated into the further development of a comprehensive, cross-layer approach can be achieved.

ii. *Secure Routing in Wireless Ad hoc Networks*

Wireless ad hoc networks routing and wire-line networks cannot rely on dedicated routers. This functionality is simple terminals, as well as routers for other nodes that work is spread out over all the nodes. Data routing face many problems, such as providing a secure environment for networking and for the purposes of possible security attacks experienced temporary special. Ad hoc networks are the most popular routing protocols do not comprise of security aspects. Ad hoc wireless networks from security attacks, and especially attacks at the network layer of the defense, some of the requirements [20] should fulfill. Complete missions and the threat of a temporary wormhole attack against the disabled can disrupt communications. Based on the identification of a number of proposals for the use of wormhole packets.

Different approaches are very security-conscious in wireless ad hoc networks which have been proposed to achieve the security. In Table -1 it shows the most important security-strengthening properties awareness which drives the appropriate techniques to solve the following implementation for the various mechanisms of security aware routing protocols (SWRP).

Table 1 : Secure aware routing properties and techniques

Authenticity	Password, certificate
Authorization	Credentials
Integrity	Digest, digital signature
Confidentiality	Encryption
Non-repudiation	Changing of digital Signatures
Timeliness	Timestamp
Ordering	Sequence number

Many security routing protocols are discussed briefly in the following subsections.

SRP: Secure Routing Protocol (SRP) [21] is regarding the information to disrupt the process of the discovery, the acquisition of the guarantee to protect against attacks that can be applied to a multitude of reactive routing protocols. Either way, replies to compromise or be rejected again or ever reach the node back to the trial, the fabrication are protocol guarantees.

SAR : This protocol[22] aware of the ad hoc routing protocol security metric to define the level of trust and security attributes which are taken into account in the routing. And significant levels of trust in the hierarchy of levels of trust between the nodes can be defined. Nodes with the high level of trust among themselves and with the distribution of a common key encryption / decryption keys for the Notes equal to the share of each trust level. However, the contract for a different level of security in the network increases the total number of keys to different keys.

SEAD: It is an efficient ad hoc distance vector operation for safe destination protocol-distance gradient vector. Vector creates DOS attacks and resource calculation (DSDV) drives Protocol [23] is based on. SEAD DSDV-SQ Operation protocol and the sequence number and operating table update message was inspired to deal with attackers that different industry metric. To secure this DSDV-SQ [24] operation protocol of SEAD not rely on each side to implement and expensive asymmetric cryptographic hash chain on art. SEAD operation using a hash table implemented security mechanisms chain features updated message sequence number and the metric is correct. The implementation mechanism to ensure the identity of the client, or the broadcast authenticates the sender information on SEAD attempt to remove malicious nodes.

ARAN: Depending on the situation ARAN cryptographic certificates, temporary ad hoc networks and the power of the routing protocol is to prevents from the malicious activities with the support of an trusted third party. Minimum safekeeping policy, reliability of messages, identity authentication and non-repudiation of a necessary from end-to-end authentication for passed and initial certification process implementation [25].

ARIADNE: On-demand safe operation Protocol of this is DSR-based highly efficient symmetric cryptography [26] only stay on. Protocol required that a genuine key to our view that this must be some. Each node of the network is the same in each of the authentic and genuine way of finding each chain element nodes to nodes (a node between the source and) must share a secret key. ARIADNE message authentication code (MAC) and the joint chief operating point provides authentication message. However, except for the higher version, wormhole does not protect against attacks.

S-AODV: Security-aware AODV protocol single malicious nodes [27] Therefore, efficient solution to eliminate the black hole attack. Malicious intermediate nodes, it was the shortest route to the destination because of advertising that black-hole problem. Or dealing with the limited means of generating e-solutions proposed by malicious packets to an intermediate node has been tested by the neighbors realized. S-AODV Protocol each intermediate node can be assumed that all transit operators ensure packets. Control Message Originator of South Africa's signature and the final part of the hash chain appends. Network cryptographically signed message headers and the second and intermediate

hash confirmed. 'S-AODV is unable to deal with malicious headers to control the working group, including a significant overhead.

VI. Secure Energy Optimization Routing in Wireless Communication

Internal attacks are ineffective or compromised nodes before using a global shared key security structures. Therefore, fair wormholes and internal attacks to identify more sophisticated security mechanisms, and to protect the malicious headers. Safe and secure operation routing that can be used to enhance the security WSN. In this section, we have selected the operation of routings for secure networks. Parts in the preceding are well know for the power of information solutions to the solutions.

a) SERP: Secure Energy Efficient Routing Protocol

Wireless Sensor Networks routing protocol for the safe, energy efficient is described in SERP – Secure energy efficient routing [25]. The main objective of this protocol is to limited base station power requirement with authentication and confidential data from the sensors to provide a robust transmission. It is relatively static sensor devices which are deployed in densely dedicated to WSNs.

The three key aims were considered during the scheme of the SERP as follows

- To ensure the efficient transmission of power to the network is to know the structure, and the maximum lifetime to the end of the network.
- Secure communications nodes should be able to identify the incorrect intrusion reports.
- Strong and resilient transmission failure of any node can greatly hamper the performance of a network.

Energy savings mechanism based on the selected nodes are disabled transceivers radio. The two main states of the nodes in a network to perform: Non forwarding - forwarding transceiver, switch off - both transceiver and sensing devices which are switched. The backbone of the structure of the network, has been the assumption that all the headers are either directed or in non-states. But while the active sensing device nodes forwarding state of their radio transceivers. On the other hand, forwarding nodes keep both the radio and the active sensing device. All the nodes to perceive the environment, and in any event not later identify nodes forwarding the data to the base station via a selected route nodes and broadcast on their radio signal ranges.

b) EENC: Energy Efficiency Routing with Node Compromised Resistance

Node is compromised immunity is a novel energy efficient routing protocol proposed by K Lin et al [28] as EENC. It describes that EENC compromised nodes under the situation of bypasses and corresponding energy intake, improves the accuracy of the packets. Reinforcement knowledge established on ant-colony optimization routing tables are used to the complete. All nodes in the network are assigned with a trust Likewise, such as multiple behavior is based on the characteristics of the computed value. A one-hop neighbor of each node in a sensor network calculates the value of the trust. The idea of EENC is to provide security for low energy consumption and manage its energy resources.

This protocol EENC was evaluated through simulation. The performance metric to consider life and network packets correctly receives rate included. The EENC performance compared with other operations algorithms, i.e., DRP and MTRP are described [29] and presents the results of simulation of EENC operating through the trans- mission line can often compromised headers [29] EENC is to ensure that the energy efficiency performance was observed, that the estimated lifetime testing and successful packet delivery ratio and a higher DRP for more EENC received MTRP.

c) Location-based Power Conservation outline

In [17] Location Based Energy Conservation Program (LBPC) was discussed by authors. They suggested that the power consumption reduction algorithm in MANET. Such protocol transmission range of adjustment for the nearest neighbors is the first Hop neighbors and arbitrary detachment between the first uses of location information provided by GPS fitted to obtain general information about the distance. Two types of algorithms based on the results of the simulation are presented in the floods, which varied from 10-50% ratio showed an energy conservation. This is a significant amount of energy conservation, and the stored power adjustments as a result of a variety of network transmission range are done. However, the average distance to the neighboring transmission range is equal to the ratio of low to provide other performance parameters, but high in energy conservation.

d) SPAN: Energy Efficient Coordination Algorithm for Topology Maintenance

SPAN protocol, which reduces power consumption without reducing network connectivity also code named to ad hoc multi-hop wireless networks for the distribution of synchronization technique [18]. SPAN is coordinated by the cycle of “stay and sleep-awake" between the nodes and the ad-hoc multi-hop data packet performs routing within the network, while the other nodes are in power redeemable approach and occasionally to check if they will awaken and become a coordinator. During coordinator election every node in the network can adaptively become a coordinator and rotating them in time to decide whether or not to use a random back-off delay, the process is done by the SPAN. Back off delay for a node to other nodes in the neighborhood of the delay and the number of nodes is a function of the amount of remaining power. Network

connectivity not only is to protect the approach adopted in SPAN, it also preserves the ability to reduce latency and provides significant energy savings. Node density decreases only slightly increases as the size of the power saving provided by SPAN. Practically nodes wake up and listen for traffic from advertising in the current run of SPAN, features energy-saving, can be used [19].

e) Power-aware Routing Protocol

Power awareness Routing (PAR) [21] is maximizes the life span of the network and, hence, the source of the data packets transmitted during the process of setting up the route to the destination, choose less congested and more stable way to reduce power consumption by providing energy efficient routes. PAR protocols on the three parameters are the accumulated energy of a way, the status of the battery's life and the type of data to be transmitted. PAR time to focus on the core metrics are chosen path, hence, less traffic for the delivery of data is considered to be more stable. That provided different ways for different type of data transfer, network lifetime are increased. PAR simulation results from the energy-related performance metrics to the different ways in high mobility scenarios, such as DSR [22] and AODV [23] shows that outperforms the relevant protocol. However, PAR suffers increased latency during data transfer, but it goes a long way, and found enormous energy savings.

VII. Conclusion

In this paper, the mobile ad-hoc network routing security solutions in energy conservation issues and provides an overview of the study of the protocols. Due to the lack of infrastructure for wireless networks and the dynamic and transient nature of the relationship between network nodes, designers, especially prepared to impose additional challenges. Advanced security mechanisms, security must be designed to achieve the goals and they are effective. Ad-hoc functionality to provide a secure link layer security features are intended to be embedded in the equipment. Another challenge is preventing the efficient use of computing resources, computing harmful. Research in the field of authentication and key management to be efficient in terms of computational burden, which focuses on the design of the cryptographic algorithms. These protocols are available in various performance demands and proposals identified by the use of force against the parameters of this exhibition show the maximum effect. The study describes the achievement of high power conservation without compromising other performance metrics in MANET which provides for the performance demands of individual protocols. In the future, we intentionally designed to deliver the perfect blend of MANETs with some metrics for the performance demands with the intention to use the proposed protocols.

References Références Referencias

1. Patwardhan, A., Parker, J., Joshi, A., Karygiannis, A., and Iorga, M., "Secure Routing and Intrusion Detection in Ad hoc Networks," 3rd IEEE International Conference on Pervasive Computing and Communications, Kauaii Island, Hawaii, March 2005
2. K. Sanzgiri, D.La Flamme, B.Dahill, B.N. Levine, C.Shields, and E.M. Belding-Royer, "Authenticated Routing for Ad Hoc Networks," Proceedings of IEEE Journal on Selected Areas in Communications, vol. 23, no. 3, March 2005.
3. M. Rahman, S. Sampalli, and S. Hussain, "A robust pair-wise and group key management protocol for wireless sensor network," in GLOBECOM Workshops (GC Wkshps), 2010 IEEE, Miami, FL, 2010, pp. 1528-1532.
4. M. El-Saadawy and E. Shaaban, "Enhancing S-LEACH security for wireless sensor networks," in Electro/Information Technology (EIT), 2012 IEEE International Conference on, 2012, pp. 1-6.
5. H. Soroush, M. Salajegheh, and T. Dimitriou, "Providing transparent security services to sensor networks," in Communications, 2007. ICC'07. IEEE International Conference on, Glasgow, 2007, pp. 3431-3436.
6. Anuradha Garg, Ajay Tiwari, Hemant Kumar Garg, "A Secure Energy Efficiency Routing Approach In Wireless Sensor Networks", International Journal of Engineering and Advanced Technology (IJEAT) , Volume-2, Issue-3, February 2013
7. E. Niewiadomska-Szynkiewicz, P. Kwaœniewski, and I. Windyga, "Comparative study of wireless sensor networks energy-efficient topologies and power save protocols", J. Telecom. Inform. Technol., no. 3, pp. 68–75, 2009.
8. K. Sharma, M. K. Ghose, D. Kumar, "A comparative study of various security approaches used in wireless sensor networks", Int. J. Adv. Sci. Technol., vol. 17, pp. 31–44, 2010.
9. M. Ahmad, M. Habib, and J. Muhammad, "Analysis of security protocols for Wireless Sensor Networks", in Proc. 3rd Int. Conf. Comp. Res. Develop. ICCRD 2011, Shanghai, China, 2011, vol. 2, pp. 383–387.
10. Perkins, C. E. and Bhagwat, P., "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," Proceedings of SIGCOMM 1994, 1994
11. Yi, S., Naldurg, P., and Kravets, R., "A Security-Aware Routing Protocol for Wireless Ad hoc Networks," 6th World Multi-Conference on Systemics, Cybernetics and Informatics (SCI 2002), 2002
12. Zhang, Y. and Lee, W., "Intrusion Detection in Wireless Ad hoc Networks," Mobicom'00, Boston, MA, USA, 2000

13. Wai, F. H., Aye, Y. N., and James, N. H., "Intrusion Detection in Wireless Ad- Hoc Networks," CS4274 Introduction to Mobile Computing, term paper, School of Computing, National University of Singapore, 2005.
14. Y.Sun, Z.Han and K.J.R.Liu, "Defense of trust management vulnerabilities in distributed networks," IEEE Communications Magazine, vol. 46, issue 2, pp.112-119, February 2008.
15. L. Gheorghe, R. Rughinis, R. Deaconescu, and N. Tapus, "Authentication and Anti-replay Security Protocol for Wireless Sensor Networks," in Systems and Networks Communications (ICSNC), 2010 Fifth International Conference on, Nice, France, 2010, pp. 7-13.
16. Mike Burmester and Breno de Medeiros, "On the Security of Route Discovery in MANETs", IEEE Transactions On Mobile Computing,March 1, 2008.
17. E. Ahmed, K. Samad, W. Mahmood, "Cluster-based Intrusion Detection (CBID) Architecture for Mobile Ad Hoc Networks," Aus CERT2006 R&D Stream Program, Information Technology Security Conference, May 2006.
18. Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu and Lixia Zhang, "Security in mobile ad hoc networks: Challenges and solutions," IEEE Wireless Communications, vol. 11, pp. 38-47, Feb., 2004.
19. K.Sanzgiri, D.LaFlamme, B. Dahill, B.N.Levine, C.Shields, and E.M.Belding-Royer, "Authenticated Routing for Ad Hoc Networks," Proceedings of IEEE Journal on Selected Areas in Communications, vol. 23, no. 3, March 2005.
20. Y.C.Hu, A.Perrig, and D.B.Johnson, "Ariadne: A Secure On- Demand Routing Protocol for Ad Hoc Networks," Proc. MobiCom'02, Atlanta, GA, pp. 12-13 September 2002.
21. B.Wu, J.Chen, J.Wu, and M.Cardei, "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks," Wireless/Mobile Network Security, Springer, vol. 17, 2006.
22. D. Balfanz, D. Smetters, P. Stewart, and H. Wong. Talking to Strangers: Authentication in Ad hoc Wireless Networks. In Proceedings of the Symposium on Network and Distributed Systems Security (NDSS '02), San Diego, California, February 2002.
23. Th. Clausen et al., "Optimized Link State Routing Protocol," IETF Internet draft, draft-ietfmanet-olsr-11.txt, July 2003.
24. P. Papadimitratos and Z. Haas, "Secure routing for mobile ad hoc networks,. in Proc. SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), 2002.
25. J. Hall, M. Barbeau, and E. Kranakis, .Enhancing intrusion detection in wireless networks using radio frequency ngerprinting,. in IASTED International Conference on Communications, Internet, and Information Technology, 2004, St. Thomas, US Virgin Islands, 2004, pp. 201.206.
26. A. K. Pathan and C. S. Hong, "SERP: secure energy-efficient routing protocol for densely deployed wireless sensor network", Annales des Telecomm., pp. 529–541, 2008.
27. K. Lin, Ch. F. Lai, X. Liu, and X. Guan, "Energy efficiency routing with node compromised resistance in wireless sensor networks", Mob. Netw. Appl., vol. 17, pp. 75–89, 2012.
28. Z. Yu and Y. Guan, "A dynamic en-route scheme for filtering false data injection in wireless sensor networks", in Proc. 25th IEEE Int. Conf. Com. Commun. INFOCOM 2006, Barcelona, Spain, 2006, pp. 1–12.
29. A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. Culler, "SPINS: security protocols for sensor networks", Wirel. Netw., vol. 8, no. 5, pp. 521–534, 2002.
30. C. Karlof, N. Sastry, and D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks", in Proc. 2nd Int. Conf. Embedded Networked Sensor Sys., Baltimore, MD, USA, 2004, pp. 162–175.
31. Ajina A, "Energy Efficient, Power Aware Routing Algorithm For Sensor Network". International Journal of Computer Theory and Engineering, Vol.3, No.1.1793-8201, February-2011.

This page is intentionally left blank