Global Journals LaTeX JournalKaleidoscope™
Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

A Trustful Routing Protocol for Ad-hoc Network

Dr. Mahendra Kumar Mishra[1]

[1]

Received: 13 March 2011 Accepted: 7 April 2011 Published: 19 April 2011

Abstract

Mobile Ad-hoc Network (MANET) is a wireless system that comprises mobile nodes. It is usually referred to a decentralized autonomous system. Self configurability and easy deployment feature of the MANET resulted in numerous applications in this modern era. Its routing protocol has to be able to cope with the new challenges that a MANET creates such as nodes mobility, security maintenance, and quality of service, limited bandwidth and limited power supply. These challenges set new demands on MANET routing protocols. With the increasing interest in MANETs, there has been a greater focus on the subject of securing such networks. However, the majority of these MANET secure routing protocols did not provide a complete solution for all the MANETs? attacks and assumed that any node participating in the MANET is not selfish and that it will cooperate to support different network functionalities. My thesis strategy is to choose one of the secure routing protocols According to its security-effectiveness, study it and analyze its functionality and performance. The authenticated routing for ad hoc networks (ARAN) secure routing protocol was chosen for analysis. Then, the different existing cooperation enforcement schemes were surveyed so that to come up with a reputation-based scheme to integrate with the ARAN protocol. The result of that integration is called: Trustful-ARAN. Consequently, the ARAN is capable of handling both selfish and malicious nodes? attacks. The improvement is obtained at the cost of a higher overhead percentage with minimal increase in the average number of hops. The Trustful-ARAN proves to be more efficient and more secure than normal ARAN secure routing protocol in defending against both malicious and authenticated selfish nodes.

Index terms— MANE T, ARAN, Routing Protocols.

1 Introduction

ireless networking is an emerging technology that allows users to access information and services electronically, regardless of their geographic position.

The use of wireless communication between mobile users has become increasingly popular due to recent performance advancements in computer and wireless technologies. This has led to lower prices and higher data rates, which are the two main reasons why mobile computing is expected to see increasingly widespread use and applications. There are two distinct approaches for enabling wireless communications between mobile hosts. The first approach is to use a fixed network infrastructure that provides wireless access points. In this network, a mobile host communicates with the network through an access About-Department of Computer Science Engineering Radharaman Institute of Technology & Science Bhopal, M.P., India point within its communication radius. When it goes out of range of one access point, it connects with a new access point within its range and starts communicating through it. An example of this type of network is the cellular network infrastructure. A major problem of this approach is handoff, which tries to handle the situation when a connection should be smoothly handed over from one access point to another access point without noticeable delay or packet loss.

Another issue is that networks based on a fixed infrastructure are limited to places where there exist such network infrastructures [1] and [4].

The second approach which is the focus of this thesis research is to form a wireless ad hoc network among users wanting to communicate with each other with no pre-established infrastructure. Laptops and personal digital assistants (PDAs) that communicate directly with each other are examples of nodes in an ad hoc network. Nodes in the ad-hoc network are often mobile, but can also consist of stationary nodes. Each of the nodes has a wireless interface and communicates with others over either radio or infrared channels.

Wireless ad-hoc networks can be deployed in areas where a wired network infrastructure may be undesirable due to reasons such as cost or convenience. It can be rapidly deployed to support emergency requirements, short-term needs, and coverage in undeveloped areas. So there is a plethora of applications for wireless ad-hoc networks. As a matter of fact, any day-to-day application such as electronic email and file transfer can be considered to be easily deployable within an ad hoc network environment. Also, we need not emphasize the wide range of military applications possible with ad hoc networks. Not to mention, the technology was initially developed keeping in mind the military applications, such as battlefield in an unknown territory where an infrastructure network is almost impossible to have or maintain. In such situations, the ad hoc networks having self-organizing capability can be effectively used where other technologies either fail or cannot be deployed effectively.

In the field of mobile ad hoc networks routing protocols, there are lot of problems to be tackled such as Quality of service, power awareness, routing optimization and security issues. In this thesis, the main interest is in the security issues related to routing protocols in MANETs. So, I started researching by reading about the different research directions in this W huge field and analyzed the different existing routing protocols and their various types. I ended up interested in the AODV protocol and studied its source code. Then more interest in secure routing protocols and their different mechanism in defending against the malicious, compromised and selfish nodes in the mobile ad hoc network were developed. Existing secure routing protocols were studied such as ARAN, SAODV, SRP and others. Then, the decision to work with the ARAN protocol was taken after having read many papers about it, getting in contact with its author and doing some comparisons and analysis with other secure routing protocols. The ARAN protocol was observed to defend almost against all security attacks in MANETs. However, by doing more research in the field of MANETs, one major flaw in any of the existing secure routing protocols was discovered. This is that all of these secure routing protocols do not account for selfish nodes whether by detecting or isolating them from the network. So I decided to read about the different types of cooperation enforcement schemes in mobile ad hoc networks and then to design and integrate a reputation-based scheme with the ARAN routing protocol to end up with Reputed-ARAN that is capable of defending itself against both malicious and authenticated selfish nodes [2] and [3].

2 II.

3 Background

Security in MANET is an essential component for basic network functionalities like packet forwarding and routing. Network operation can be easily jeopardized if security countermeasures are not embedded into basic network functions at the early stages of their design. In mobile ad hoc networks, network basic functions like packet forwarding, routing and network management are performed by all nodes instead of dedicated ones. In fact, the security problems specific to a mobile ad hoc network can be traced back to this very difference. Instead of using dedicated nodes for the execution of critical network functions, one has to find other ways to solve this because the nodes of a mobile ad hoc network cannot be trusted in this way. In the following section, the different types of attacks in MANETs will be presented.

4 ? Attacks targeting Routing Protocols

There are basically two types of security threats to a routing protocol, external and internal attackers. An external attacker can be in the form of an adversary who injects erroneous information into the network and cause the routing to stop functioning properly. The internal attacker is a node that has been compromised, which might feed other nodes with incorrect information.

? Malicious and Selfish Nodes in MANETs Malicious nodes can disrupt the correct functioning of a routing protocol by modifying routing information, by fabricating false routing information and by impersonating other nodes. On the other side, selfish nodes can severely degrade network performances and eventually partition the network by simply not participating in the network operation.

In existing ad hoc routing protocols, nodes are trusted in that they do not maliciously tamper with the content of protocol messages transferred among nodes. Malicious nodes can easily perpetrate integrity attacks by simply altering protocol fields in order to subvert traffic, deny communication to legitimate nodes (denial of service) and compromise the integrity of routing computations in general. As a result the attacker can cause network traffic to be dropped, redirected to a different destination or to take a longer route to the destination increasing communication delays [2] and [5].

A more subtle type of active attack is the creation of a tunnel (or wormhole) in the network between two colluding malicious nodes linked through a private connection bypassing the network. This exploit allows a node

to short-circuit the normal flow of routing messages creating a virtual vertex cut in the network that is controlled by the two colluding attackers.

In the figure **??**, M1 and M2 are malicious nodes collaborating to misrepresent available path lengths by tunneling route request packets. Solid lines denote actual paths between nodes, the thin line denotes the tunnel, and the dotted line denotes the path that M1 and M2 falsely claim is between them. Let us say that node S wishes to form a route to D and initiates route discovery.

5 Figure 1 Wormhole Attack

When M1 receives a RDP from S, M1 encapsulates the RDP and tunnels it to M2 through an existing data route, in this case {M1?A?B?C?M2}. When M2 receives the encapsulated RDP, it forwards the RDP on to D as if it had only traveled {S?M1?M2?D}. Neither M1 nor M2 update the packet header to reflect that the RDP also traveled the path {A?B?C}. After route discovery, it appears to the destination that there are two routes from S of unequal length: {S?A?B?C?D} and {S?M1?M2?D}. If M2 tunnels the RREP back to M1, S would falsely consider the path to D via M1 a better choice (in terms of path length) than the path to D via A. Another exposure of current ad hoc routing protocols is due to node selfishness that results in lack of cooperation among ad hoc nodes. A selfish node that wants to save battery life, CPU cycles and bandwidth for its own communication can endanger the correct network operation by simply not participating in the routing protocol or by not forwarding packets and dropping them whether control or data packets. This type of attack is called the blackhole attack. Current Ad Hoc routing protocols do not address the selfishness problem and assumes that all nodes in the MANET will cooperate to provide the required network functionalities.

6 Routing Protocols' Security Requirements

To solve the security issue in an ad hoc network and make it secure we have to look at a number of requirements that have to be achieved. These requirements are: availability, confidentiality, integrity, authentication and non-repudiation.

?Availability: the network must at all times be available to send and receive messages despite if it is under attack. An attack can be in the form of a denial of service or an employed jamming to interfere with the communication. Other possible threats to the availability are if an attacker disrupts the routing protocol or some other high-level service and disconnects the network. The node itself can also be the problem to availability. This is if the node is selfish and will not provide its services for the benefit of other nodes in order to save its own resources like, battery power.

?Confidentiality: provides secrecy to sensitive material being sent over the network. This is especially important in a military scenario where strategic and tactical information is sent. If this information would fall into enemy hands it could have devastating ramifications.

? Integrity: ensures that messages being sent over the network are not corrupted. Possible attacks that would compromise the integrity are malicious attacks on the network or benign failures in the form of radio signal failures.

?Authentication: ensures the identity of the nodes in the network. If A is sending to B, A knows that it is B who is receiving the message. Also B knows that it is A who is sending the message. If the authentication is not working, it is possible for an outsider to masquerade a node and then be able to send and receive messages without anybody noticing it, thus gaining access to sensitive information.

? Non-repudiation: makes it possible for a receiving node to identify another node as the origin of a message. The sender cannot deny having sent the message and are therefore responsible for its contents. It is particularly useful for detection of compromised nodes. However, because there are so many threats to protect from, there can not be a general solution to them all. Also different applications will have different security requirements to take into consideration. As a result of this diversity, many different approaches have been made which focus on different parts of the problems. In the coming section, a comparison of some of the existing secure mobile ad hoc routing protocols with respect to most of the fundamental performance parameters will be given [1] and [4] and [6].

7 Authenticated Routing for Ad Hoc Networks Protocol (ARAN)

One of the secure mobile ad hoc networks protocols, which is Authenticated routing for ad hoc networks (ARAN) is analyzed. Such protocol is classified as a secure reactive routing protocol, which is based on some type of query-reply dialog. That means ARAN does not attempt to continuously maintain the up-todate topology of the network, but rather when there is a need, it invokes a function to find a route to the destination. In the following subsections, the details of the different phases of the ARAN secure routing protocol are presented. Furthermore, appendix B presents documentation for all the functions of ARAN secure mobile ad hoc network routing protocol.

8 Authenticated Routing for Ad Hoc Networks

The ARAN secure routing protocol proposed in recent and uses cryptographic certificates to prevent and detect most of the security attacks that most of the ad hoc routing protocols face. This protocol introduces authentication, message integrity and non-repudiation as part of a minimal security policy for the ad hoc environment.

ARAN consists of a preliminary certification process followed by a route instantiation process that guarantees end-to-end authentication. Thus, the routing messages are authenticated end-to-end and only authorized nodes participate at each hop between source and destination.

9 Route Maintenance

When no traffic has occurred on an existing route for that route's lifetime, the route is simply deactivated in the routing table. Data received on an inactive route causes nodes to generate a Route Error (RERR) message. Also, nodes use RERR messages to report links in active routes that are broken due to node movement. Of course, all RERR messages are signed.

On the other hand, it is extremely difficult to detect when RERR messages are fabricated for links that are truly active and not broken. That is why having messages signed prevents impersonation and enables non-repudiation. So a node that transmits a large number of RERR messages, whether the RERR messages are valid or fabricated should be avoided.

In the event that a certificate needs to be revoked, the trusted certificate server, T, sends a broadcast message to the ad hoc network announcing the revoked node. And any node receiving this message rebroadcasts it to its neighbors. Moreover, revocationnotices need to be stored until the revoked certificate expire normally [7] and [8]. An analysis of the robustness of the Authenticated Routing for Ad Hoc Networks in the presence of the different attacks introduced in earlier sections is given: ? Unauthorized participation: Since all ARAN packets must be signed, a node cannot participate in routing without authorization from the trusted certificate server. This access control therefore rests in the security of the trusted authority, the authorization mechanisms employed by the trusted authority, the strength of the issued certificates, and the revocation mechanism. ?Spoofed Route Signaling: Route discovery packets contain the certificate of the source node and are signed with the source's private key. Similarly, reply packets include the destination node's certificate and signature, ensuring that only the destination can respond to route discovery. This prevents impersonation attacks where either the source or destination node is spoofed. ?Fabricated Routing Messages: Since all routing messages must include the sending node's certificate and signature, ARAN ensures non-repudiation and prevents spoofing and unauthorized participation in routing. ? Alteration of Routing Messages: ARAN specifies that all fields of RDP and RREP packets remain unchanged between source and destination. Since both packet types are signed by the initiating node, any alterations in transit would be detected, and the altered packet would be subsequently discarded. Thus, modification attacks are prevented in ARAN.

Denial-of-Service Attacks: Denial-of-service (DoS) attacks can be conducted by nodes with or without valid ARAN certificates. In the certificate-less case, all possible attacks are limited to the attacker's immediate neighbors because unsigned route requests are dropped. However, nodes with valid certificates can conduct effective DoS attacks by sending many unnecessary route requests and they will go undetected as the current existing ARAN protocol cannot differentiate between legitimate and malicious RREQs coming from authenticated nodes. It is clear from the above mentioned security analysis of the ARAN protocol that ARAN is a secure MANET routing protocol providing authentication, message integrity, confidentiality and non-repudiation by using certificates infrastructure. As a consequence, ARAN is capable of defending itself against spoofing, fabrication, modification, DoS and disclosure attacks. However, erratic behavior can come from a malicious node, which will be defended against successfully by existing ARAN protocol, and can also come from an authenticated node. The currently existing ARAN secure routing protocol does not account for attacks that are conducted by authenticated selfish nodes as these nodes trust each other to cooperate in providing network functionalities. This results in that ARAN fails to detect and defend against an authenticated selfish node participating in the mobile ad hoc network. Thus, if an authenticated selfish node does not forward or intentionally drop control or data packets, the current specification of ARAN routing protocol cannot detect or defend against such authenticated selfish nodes. This weakness in ARAN specification will result in the disturbance of the ad hoc network and the waste of the network bandwidth. A solution is proposed to account for this type of attack [1] and [2] and [4] and [7].

10 Proposed Technique

Performance of Mobile Ad Hoc Networks is well known to suffer from free-riding, selfish nodes, as there is a natural incentive for nodes to only consume, but not contribute to the services of the system. The definition of selfish behavior and the newly designed reputationbased scheme, to be integrated with normal ARAN routing protocol ending up having Reputed-ARAN, are presented.

11 Main Idea of the Reputation System

In the proposed reputation scheme, all the nodes in the mobile ad hoc network will be assigned an initial value of null (0) as in the Ocean reputation-based scheme. Also, the functionality of the normal ARAN routing protocol in the authenticated route setup phase will be modified so that instead of the destination unicasts a RREP to the first received RDP packet of a specific sender only, the destination will unicast a RREP for each RDP packet it receives and forward this RREP on the reverse-path. The next-hop node will relay this RREP. This process continues until the RREP reaches the sender. After that, the source node sends the data packet to the node with the highest reputation. Then the intermediate node forwards the data packet to the next hop with the highest reputation and the process is repeated till the packet reaches its destination. The destination acknowledges the data packet (DACK) to the source that updates its reputation table by giving a recommendation of (+1) to the first hop of the reverse path. All the intermediate nodes in the route give a recommendation of (+1) to their respective next hop in the route and update their local reputation tables. If there is a selfish node in the route, the data packet does not reach its destination. As a result, the source does not receive any DACK for the data packet in appropriate time. So, the source gives a recommendation of (-2) to the first hop on the route. The intermediate nodes also give a recommendation (-2) to their next hop in the route up to the node that dropped the packet. As a consequence, all the nodes between the selfish node and the sender, including the selfish node, get a recommendation of (-2). The idea of giving (-2) to selfish nodes per each data packet dropping is due to the fact that negative behavior should be given greater weight than positive behavior. In addition, this way prevents a selfish node from dropping alternate packets in order to keep its reputation constant. This makes it more difficult for a selfish node to build up a good reputation to attack for a sustained period of time. Moreover, the selfish node will be isolated if its reputation reached a threshold of (-40) as in the Ocean reputation-based scheme.

The proposed protocol is structured into the following four main phases, which are explained in the subsequent subsections:

? Route Lookup Phase ? Data Transfer Phase ? Reputation Phase ? Timeout Phase

12 Route Lookup Phase

This phase mainly incorporates the authenticated route discovery and route setup phases of the normal ARAN secure routing protocol. In this phase, if a source node S has packets for the destination node D, the source node broadcasts a route discovery packet (RDP) for a route from node S to node D. Each intermediate node interested in cooperating to route this control packet broadcasts it throughout the mobile ad hoc network; in addition, each intermediate node inserts a record of the source, nonce, destination and previous-hop of this packet in its routing records. This process continues until this RDP packet reaches the destination. Then the destination unicasts a route reply packet (RREP) for each RDP packet it receives back using the reverse-path. Each intermediate node receiving this RREP updates its routing table for the next-hop of the route reply packet and then unicasts this RREP in the reverse-path using the earlier-stored previous-hop node information. This process repeats until the RREP packet reaches the source node S. Finally, the source node S inserts a record for the destination node D in its routing table for each received RREP. In the below figures, the route lookup phase is presented in details, illustrating the two phases of it, the authenticated route discovery phase and the authenticated route setup phase. RDP packet sent earlier. So, the source node S chooses the highly-reputed next-hop node for its data transfer. If two next-hop nodes have the same reputation, S will choose one of them randomly, stores its information in the sent-table as the path for its data transfer. Also, the source node will start a timer before it should receive a data acknowledgement (DACK) from the destination for this data packet. Afterwards, the chosen next-hop node will again choose the highly-reputed next-hop node from its routing table and will store its information in its sent-table as the path of this data transfer. Also, this chosen node will start a timer, before which it should receive the DACK from the destination for this data packet. This process continues till the data packet reaches the destination node D. And of course in this phase, if the data packet has originated from a lowreputed node, the packet is put back at the end of the queue of the current node. If the packet has originated from a high-reputed node, the current node sends the data packet to the next highly-reputed hop in the route discovered in the previous phase as soon as possible. Once the packet reaches its destination, the destination node D sends a signed data acknowledgement packet to the source S. The DACK traverses the same route as the data packet, but in the reverse direction. In the following figures, the data transfer phase is illustrated:

13 Reputation Phase

In this phase, when an intermediate node receives a data acknowledgement packet (DACK), it retrieves the record, inserted in the data transfer phase, corresponding to this data packet then it increments the reputation of the next hop node. In addition, it deletes this data packet entry from its sent-table. Once the DACK packet reaches node S, it deletes this entry from its sent-table and gives a recommendation of (+1) to the node that delivered the acknowledgement.

14 Timeout Phase

In this phase, once the timer for a given data packet expires at a node; the node retrieves the entry corresponding to this data transfer operation returned by the timer from its sent-table. Then, the node gives a negative recommendation (-2) to the next-hop node and deletes the entry from the sent-table. Later on, when the intermediate nodes' timers up to the node that dropped the packet expire, they give a negative recommendation to their next hop node and delete the entry from their sent-table. As a consequence, all the nodes between the selfish node and the sender, including the selfish node, get a recommendation of (-2). Now, if the reputation of the next-hop node goes below the threshold (-40), the current node deactivates this node in its routing table and sends an error message RERR to the upstream nodes in the route. Then the original ARAN protocol handles it. Now, it is the responsibility of the sender to reinitiate the route discovery again. In addition, the node whose reputation value reached (-40) is now temporally weeded out of the MANET for five minutes and it later joins the network with a value of (0) so that to treat it as a newly joined node in the network.

15 Analysis of the proposed Reputed-ARAN

An analysis of the proposed reputation-based scheme is given by discussing different authenticated selfish nodes' forms of attacks and presenting ways of counteracting them by the introduced reputation-based scheme. ? An authenticated selfish node might make a false claim of knowing the route to a destination and generate a RREP for a destination for which it does not have a route. This attack can be foiled by the proposed reputation-based scheme routing. After receiving the data packet for the corresponding destination, this authenticated selfish node will have to drop the data packet. The sender and the intermediate nodes until this selfish node will give a negative recommendation to it. Thus, once the reputation of this selfish node falls below the threshold reputation, it will be considered as selfish and will eventually be temporary ostracized. ?An authenticated selfish node might not reveal that it knows the route to the destination by not replying to or forwarding control packets so that to save its resources, such as energy and processing power; by doing this selfish behavior, it will not be able to inflict any damage to the network as it will not be able to drop the data packets routed via other paths. To face this type of selfish attack, the proposed scheme considers the reputation value of the node asking others to forward its packets. If the packet has originated from a low-reputed node, the packet is assigned lowermost priority and if the packet has originated from a high-reputed node, the current node sends the data packet to the next hop in the route as soon as possible. Hence, these selfish nodes will see a considerable increase in network latency. So, the proposed scheme helps in encouraging the nodes to participate and cooperate in the ad hoc network effectively. ? An authenticated selfish node might promise to route data packets, but then it starts to drop all the data packets that it receives. The presented reputationbased scheme foils this attack. In such a scenario, the upstream neighbor of the node will give it a negative recommendation and the reputation of the node will be reduced. Eventually, the node will be weeded out of the network for a period of time. ?Authenticated selfish nodes might collude by giving positive recommendations to each other so that to increase their reputations. The proposed reputationbased scheme prevents this attack by having the nodes rely on their own experience rather than the experience of their peers. Although the exchange of reputation information among the nodes will make the system more robust, it is not incorporated in my scheme. This is due to that if the nodes exchange the reputations of other nodes, the target (node soliciting reputation of another node) will have to consider the credibility of the information source (node providing reputation of another node). As a result, this will imply more work for the nodes at the routing layer and will also increase the volume of the network traffic. The downside of my scheme is that an authenticated selfish node can move around the network and selectively drop packets from different neighbors without getting caught for a long time. However, eventually this selfish node will be caught. ?An authenticated selfish node might continuously drops data packets to decrease the throughput of the mobile ad hoc network. The presented scheme can prevent such attack. Since the nodes in an ad hoc network are semi-autonomous, the proposed reputation-based scheme motivates them to allocate their resources to other nodes in the network. As the sender relays the packet only to highly reputed neighbors, it reduces the risk that its neighbors will intentionally drop the packet. The neighbors in turn forward the packets to nodes that have a high reputation with them. As a result, the number of packets intentionally dropped is reduced and the throughput of the system rises. ? An authenticated well-behaved node might become a bottleneck since in the presented reputation-based scheme the node with the highest reputation is selected as the next hop by its neighbor. As a result, the nodes with higher reputations will become overloaded, while the other nodes become totally free. This problem is prevented in the proposed scheme as when authenticated nodes are congested and they cannot fulfill all control packets broadcasted in the MANET, they can choose not to reply to other nodes' requests in order to do their own assigned load according to their battery, performance and congestion status.

16 III.

17 Results

The below figure **??** shows the results of the network throughput of both protocols: normal ARAN and Reputed-ARAN (Trustful ARAN) with different node speed and different percentages of selfish nodes. From the above

graph, it is clear that the lack of cooperation has fatal effect on the efficient work in dramatic fall in normal ARAN's network throughput with increasing percentage of selfish nodes.

The different curves show a network of 20 nodes with different percentages of selfish nodes, from 0% up to 30%, and moving at different speeds. Here are some points that can be observed in this graph:

In the case that there are no selfish nodes in the mobile ad hoc network, both ARAN and Reputed-ARAN have almost identical network throughput values. This proves that the Reputed-ARAN protocol is as efficient as ARAN in delivering the packets and discovering routes to any destination. It can be noted that in both ARAN and Reputed-ARAN when the node movement speed rises, the network throughput diminishes as the network in general gets more fragile.

18 Effects of Selfish nodes on Network Throughput

Also, as the percentage of selfish nodes participating in the mobile ad hoc network increase, the throughput decreases because these selfish nodes tend to drop packets that they beforehand promised to forward. The outcome of dropping packets affects the normal ARAN protocol during the full life of the MANET, but in case of Reputed-ARAN, it is just affected partially as by time the selfish node will be identified and weeded out of the network. The increase of throughput of the network in the case of using Reputed-ARAN is attributed to that each node uses its local table of other nodes' reputation values in the selection of the next-hop node for establishing the data route.

Thus, the throughput of the network is reduced to 38.8% with normal ARAN, when 30% of the nodes are selfish and moving at speed of 10 m/s. However, the throughput of the network is reduced to only 63.1% with Reputed-ARAN, in the same circumstances. This proves that the Reputed g of the MANET. This graph shows the ARAN increases the network throughput by 38.5% over normal ARAN secure routing protocol.

The below figure 9 shows the results of the average route acquisition delay metric of both protocols: normal ARAN and Reputed-ARAN with different percentage of selfish nodes.

From the graph, it is clear that the newly proposed Reputed-ARAN protocol has an identical route acquisition delay as normal ARAN. This is due to that both protocols have the same steps for the discovery, setup and maintenance of the route, as no changes were done in these phases while designing the Reputed-ARAN. Also, it can be seen from the graph that in both protocols, the average route acquisition delay increases with the increase of the selfish nodes. This is due to the dropping of packets because of link failures and also because of the selfish behavior which results in reissuing a route discovery or taking a longer route to reach the destination.

IV.

19 Conclusion

The field of MANETs is rapidly growing and changing. While there are still many challenges that need to be met, it is likely that such networks will see widespread use within the next few years. One of these challenges is security. Security of mobile ad hoc networks has recently gained momentum in the research community. Due to the open nature of ad hoc networks and their inherent lack of infrastructure, security exposures can be an impediment to basic network operation and countermeasures should be included in network functions from the early stages of their design. Security solutions for MANET have to cope with a challenging environment including scarce energy and computational resources and lack of persistent structure to rely on for building trust. To my knowledge, there is no previously published work on detecting and defending against malicious and authenticated selfish nodes together in the field of MANETs' routing protocols, even in the proposed secure routing protocols.

Throughout this thesis, discussion of existing mobile ad hoc networks' routing protocols' types and their advantages and disadvantages was given and a list of existing proactive, reactive and secure MANET routing protocols was compiled. Then, the different types of attacks targeting MANET routing protocols' security were explored. Also, the difference between malicious and selfish nodes and their associated attacks were discussed and a presentation of the fundamental requirements for the design of a secure routing protocol to defend against these security breaches was given. Furthermore, a comparison between some the existing secure mobile ad hoc routing protocols was presented. Then, an in-depth talk about the Authenticated Routing for Ad Hoc Networks protocol (ARAN) as one of the secure routing protocols built following the fundamental secure routing protocols design methodology was given. Afterwards, a discussion of how ARAN defends against most of the attacks that are conducted by malicious nodes such as spoofing, fabrication, modification and disclosure ones was presented. That resulted in proving that the currently existing specification of the ARAN secure routing MANET protocol does not defend against attacks performed by authenticated selfish nodes. Thus, I moved on discussing the different existing MANET cooperation enforcement schemes by stating their types: the virtual currency-based and the reputationbased schemes. Examples of each scheme and the different issues involved in the design of each were given. That resulted in proposing a new design of a reputation-based scheme to integrate it with one of the secure routing MANET protocols, ARAN, to make it detect and defend against selfish nodes and their misbehavior. In this proposal, the different phases of the proposed reputation-based scheme were explained. Then, an analysis of the various forms of selfish attacks that the proposed reputation-based scheme defends against was presented. Also, some time was invested in surveying the different simulation packages that are used in mobile ad hoc

389 networks. Thus, the proposed design proves to be more efficient and more secure than normal ARAN secure routing protocol in defending against both malicious and authenticated selfish nodes. [1] [2] [3] [4] [5] [6] [7] [8] [9] [10]

2

Figure 1: Figure 2 :

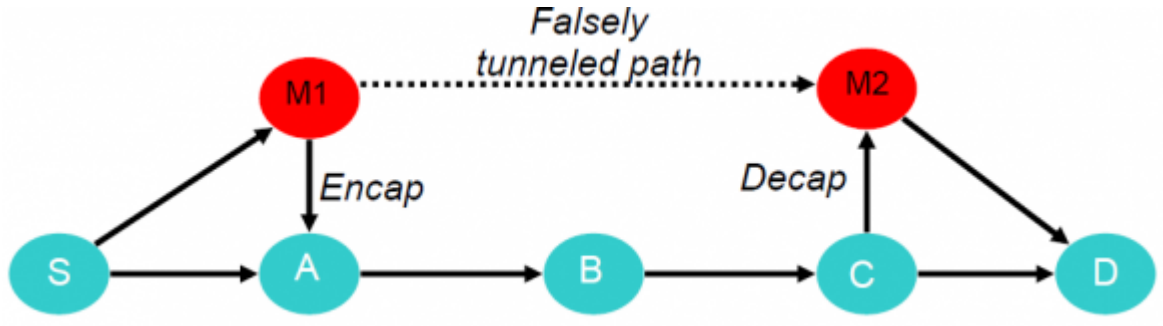
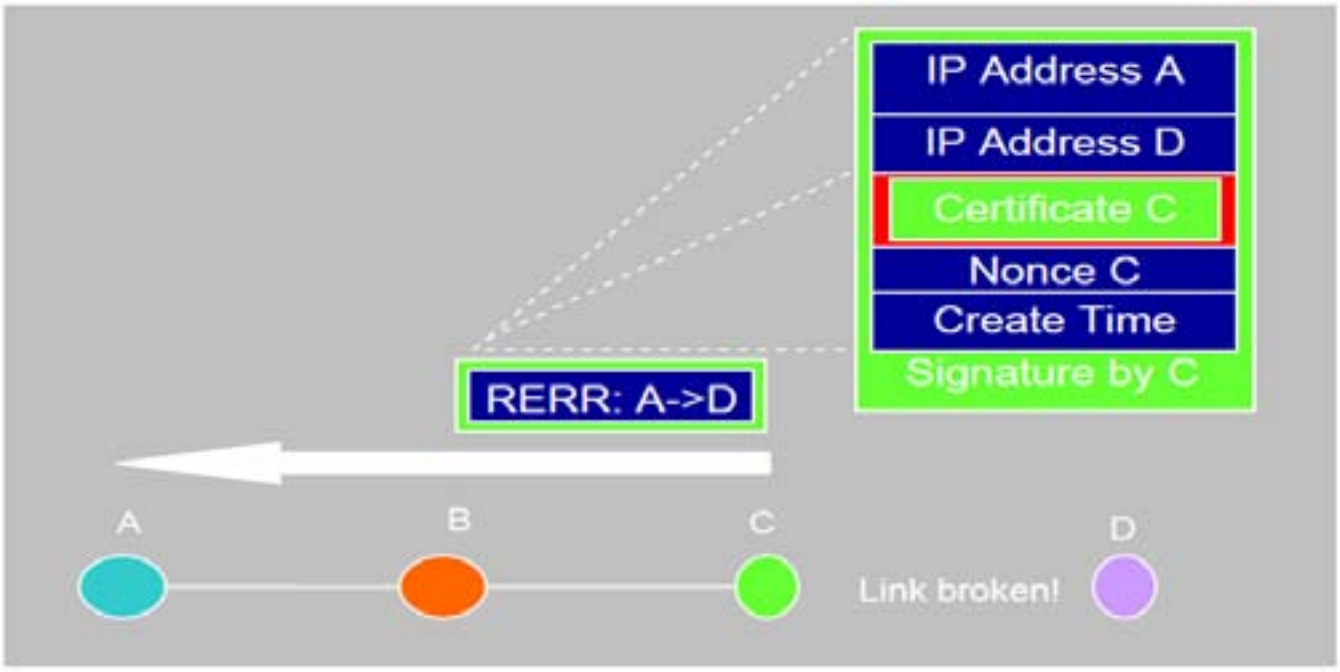


Figure 2:

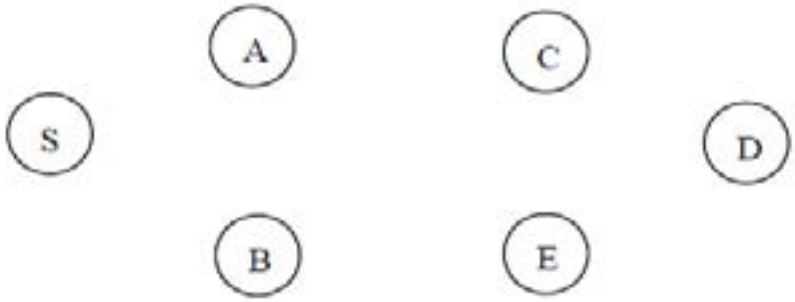
390

[1] May©2011 Global Journals Inc. (US)
[2] May©2011 Global Journals Inc. (US)
[3] May©2011 Global Journals Inc. (US)
[4] May©2011 Global Journals Inc. (US)
[5] May©2011 Global Journals Inc. (US)
[6] May©2011 Global Journals Inc. (US)
[7] May©2011 Global Journals Inc. (US)Figure 8:
[8] May©2011 Global Journals Inc. (US)
[9] May©2011 Global Journals Inc. (US)
[10] May ©2011 Global Journals Inc. (US)This page is intentionally left blank



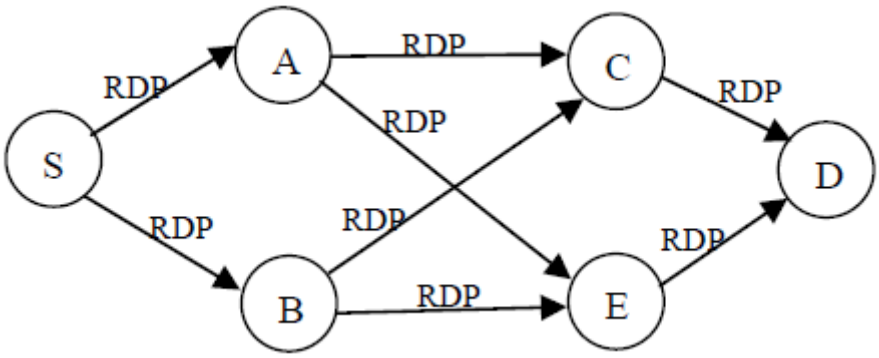
3

Figure 3: Figure 3 :



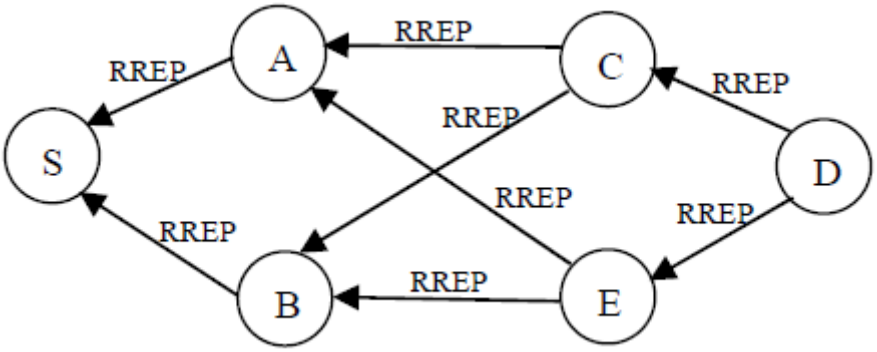
4

Figure 4: Figure 4 :



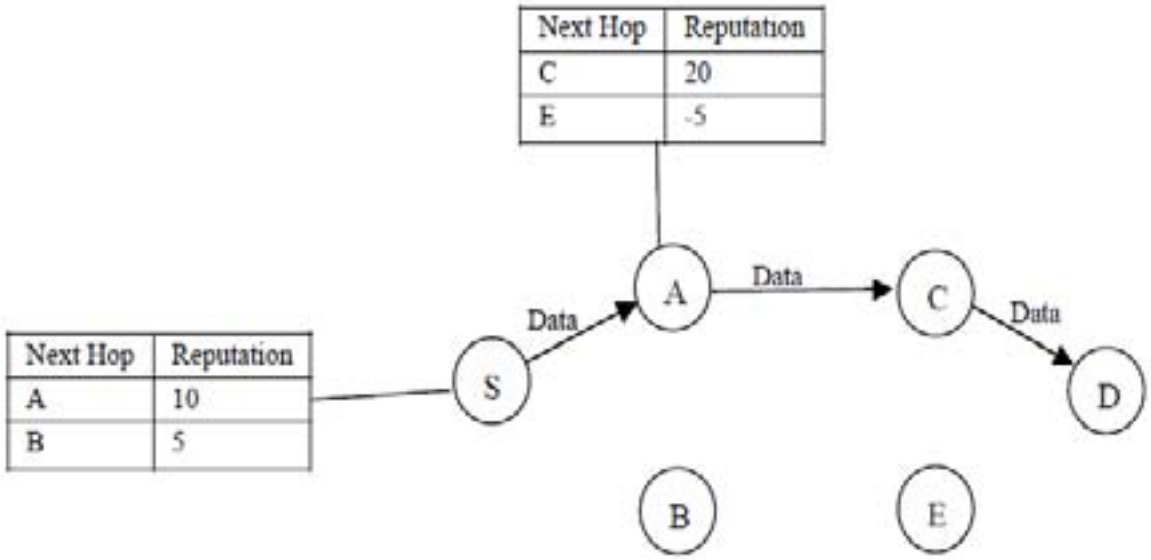
5

Figure 5: Figure 5 :



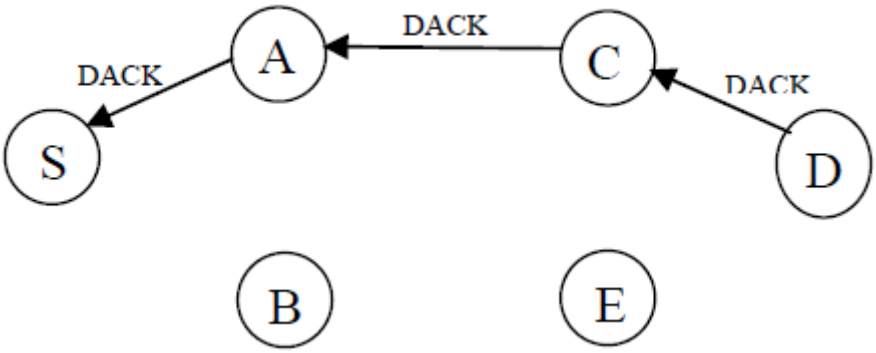
6

Figure 6: Figure 6 :



7

Figure 7: Figure 7 :



9

Figure 8: Figure 9 :

[Ni et al.] *A-Kad: an anonymous P2P protocol based on Kad network*, Yongqing Ni , Daehun Nyang , Xu Wang . IEEE 2009.

[Bhalaji et al.] *ASSOCIATION BETWEEN NODES TO COMBAT BLACKHOLE ATTACK IN DSR BASED MANET*, N Bhalaji , . A Dr , Shanmugam . IEEE 2009.

[Matthew Tan Creti et al. ()] *Multigrade Security Monitoring for Ad-Hoc Wireless Networks*, Matthew Matthew Tan Creti , Saurabh Beaman , Zhiyuan Bagchi , Yung-Hsiang Li , Lu . 2009. IEEE.

[Suganya Devi and Padmavathi] 'Performance Efficient EOMCT Algorithm for Secure Multicast Key Distribution for Mobile Adhoc Networks'. D Suganya Devi , Dr G Padmavathi . *IEEE 2009 International Conference on Advances in Recent Technologies in Communication and Computing*,

[Ren et al.] *Providing Source Privacy in Mobile Ad Hoc Networks*, Jian Ren , Yun Li , Tongtong Li . IEEE 2009.

[Jabbar et al. ()] 'REAR: Realtime Energy Aware Routing for Wireless Adhoc Micro Sensors Network'. Sohail Jabbar , Abid Ali Minhas , Raja Adeel Akhtar , Muhammad Zubair Aziz . *Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing*, 2009.

[Lavanya et al.] 'SECURED BACKUP ROUTING PROTOCOL FOR AD HOC NETWORKS'. G Lavanya , C Kumar , A Rex , Arokiaraj . *IEEE 2010 International Conference on Signal Acquisition and Processing*,

[Zhou and Haas (1999)] *Securing Ad Hoc Networks*, L Zhou , Z Haas . November/December 1999. p. .

[Pushpalakshmi et al.] 'Security aware Minimized Dominating Set based Routing in MANET'. R Pushpalakshmi , Dr A Vincent Antony , Kumar . *IEEE 2010 Second International conference on Computing, Communication and Networking Technologies*,

[Zhong et al. (2003)] 'Sprite: A simple, Cheat-proof, Credit-based System for Mobile Ad hoc Networks'. S Zhong , J Chen , Y Yang . *Proceedings of IEEE Infocom*, (IEEE Infocom) April 2003. p. .