Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 4, April 2014, pg.934 – 943

RESEARCH ARTICLE

Security Issues in MANET Routing Protocols and Their Solutions

Mahesh Kumar Kumawat (M.Tech Scholar)[1], Jitendra Singh Yadav (Assistant Professor)[2]

[1]Department of Computer Science Engineering & JECRC University, Jaipur (Rajasthan), India

[2]Department of Computer Science Engineering & JECRC University, Jaipur (Rajasthan), India

[1] kkmahesh2010@gmail.com; [2] jitendra.yadav@jecrcu.edu.in

Abstract— Mobile Ad-Hoc Networks (MANETs) are becoming increasingly popular as more and more mobile devices find their way to the public, besides "traditional" uses such as military battlefields and disaster situations. They are being used step by step in every-day stages. With this increased usage of MANETs comes the need for making the networks secure as well as efficient, something that is not readily done as many of the demands of network security conflicts. Mobile ad-hoc networks are insecure due to its open medium nature, dynamic changes in network topology, co-operative algorithms, lack of centralized monitoring point and lack of a clear line of defence. Security has become a primary concern in order to provide protected communication between mobile nodes in an enemy environment. Unlike the wired networks, the Unique characteristics of mobile ad hoc networks pose a number of nontrivial challenges to security formation, such as open peer to peer network architecture, shared wireless medium, tough resource constraints, and highly dynamic network topology. Security issues rise in many different areas including substantial security, key management, routing and intrusion detection, many of which are important to a functional MANET.

In this paper we have discussed the security issues related to the ad hoc routing protocols. The routing protocols with no proper routing function remains a key issue in ad hoc networks, the network readily will not work the way it's intentioned to. Unfortunately, routing may also be one of the most difficult areas to protect against attacks because of the ad hoc nature of MANETs. We have also discussed the main security risks involved in ad-hoc routing as well as the solutions to these problems that are exist today.

Keywords—Ad-hoc routing protocols; Routing protocol attacks; MANET security issues; Solution of routing protocol attacks; Security issues in ad-hoc routing protocols

I. INTRODUCTION

A Mobile Ad Hoc Network (MANET) is a collection of mobile nodes that cooperate and forward packets for each other. Such networks extend the fixed wireless transmission range of each node by multi-hop packet forwarding, and therefore they are ideally suitable for scenarios in which pre-deployed infrastructure support is not available. MANETs have some special characteristics such as unreliable wireless links used for communication between hosts, limited bandwidth, constantly changing network topologies, computation power and low battery power etc. Confidentiality and integrity of the data in network services

can be achieved by assuring that security issues have been met. MANET often suffers from security attacks due to its basic features like open medium, cooperative algorithms, dynamic changes in network topologies, lack of a clear line of defence, lack of centralized monitoring and management point. While these characteristics are important for the pliability of MANETs, they introduce specific security concerns that are either absent or less intense in wired networks. MANETs are permeable to various types of attacks including passive eavesdropping, impersonation, active interfering and denial-of-service.

In this paper we will discuss about the Ad-hoc routing protocols, routing protocol attacks, issues with ad-hoc routing protocols due to attacks and Solutions to Secure Routing Protocols. The routing protocols with no proper routing function remains a key issue in ad hoc networks, the network readily will not work the way it's intentioned to. Unfortunately, routing may also be one of the most difficult areas to protect against attacks because of the ad hoc nature of MANETs. We will operating the main security risks involved in ad-hoc routing as well as the solutions to these problems that are exist today.

II. SECURITY REQUIREMENTS OF MANETS

- Availability
- Authorization and Key Management
- Data Confidentiality
- Data Integrity
- Non-repudiation

III. CHARACTERISTICS OF AD-HOC ROUTING PROTOCOLS

Ad-hoc routing protocols have some special Characteristics:

- Distributed operation
- Loop freedom
- Demand-based operation
- Sleep period operation
- Unidirectional link support
- Security

IV. AD-HOC ROUTING PROTOCOLS

Routing protocols plays a important role in determining performance parameters such as packet delivery fraction, packet loss, end to end delay etc. of any ad hoc communication network. MANET routing protocols can be categorized into several parts as: table-driven/proactive, on demand driven/reactive & hybrid [Fig.1]. Depending on the routing topology table-driven are typically proactive protocols. Examples of this type include (DSDV) Destination Sequence Distance Vector. Source-initiated on demand or Reactive protocols do not periodically modify the routing information. It is transmitted to the nodes mere when essential. For Example, (DSR) Dynamic Source Routing and (AODV) Ad Hoc On Demand Distance Vector. Hybrid protocols make use of both proactive and reactive techniques. Example of this type of technique is Zone Routing Protocol (ZRP).

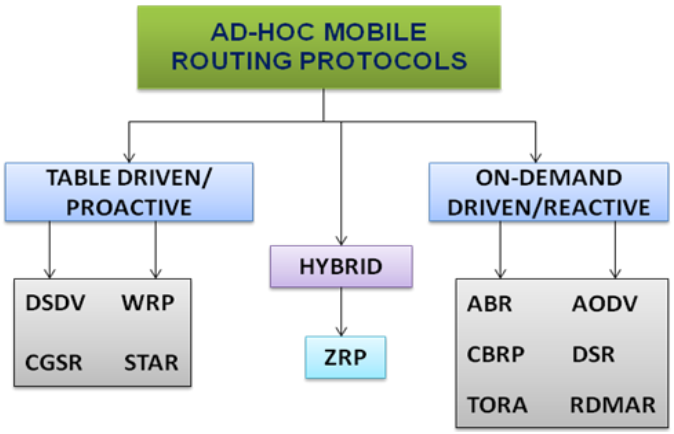

Fig 1: Routing Protocols for Mobile Ad hoc Networks

Some important Mobile Ad hoc Network routing protocols are described below:

A. Ad-hoc On Demand Distance Vector (AODV) Routing Protocol

The Ad hoc On-demand Distance Vector (AODV) is a widely used simple, efficient and effective routing protocol. It typically minimizes the number of required broadcasts by creating routes on a demand basis, when a source node wishes to route a packet to a destination node, it uses the specified route if afresh enough route to the destination node is available in its routing table. If not, it starts with a route discovery process by broadcasting the Route Request (RREQ) message to its neighbours, which is further propagated while it reaches an intermediate node with afresh enough route to the destination node specified in the RREQ ,or the destination node itself. AODV make a route using a route request / route reply query cycle. When a source node requires a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across the network. Nodes admit this packet update their information for the source node and set up backwards pointers to the source node in the route tables.

B. Dynamic Source Routing (DSR) Protocol

Dynamic Source Routing (DSR) is a type of reactive protocol. The main characteristic of DSR is source routing in which the source ever knows the complete route or path from source to destination. Route maintenance is applied to monitor correctness of established routes and to initialize route discovery if a route fails. The Dynamic Source Routing is an effortless and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. In DSR, intermedial nodes do not need to maintain the routing information.

C. Zone Routing Protocol (ZRP)

Zone Routing Protocol reduces the proactive scope to a zone entered on every node. In an incomprehensive Zone, the maintenance of routing information is easier. Also, the amount of routing information that is never used is minimized. It can be categorized as a flat protocol because the zones overlap. Hence, best routes can be determined and network congestion can be reduced. ZRP is come under the hybrid protocol category. It uses the characteristics of reactive & proactive routing protocol.

D. Destination Sequenced Distance Vector (DSDV)

In DSDV every node in the network maintains a routing table in which all of the possible destinations within the network and the number of hops to each destination are recorded. The destination node is assigned a sequentially numbered for each entry. These sequence numbers are enabled the mobile nodes to distinguish stale routes from new ones, thus avoiding the creation of routing loops. The table consistency is maintained periodically by routing table modifications in the network. Each node maintains a route to every other node in the network by Destination Sequence Distance Vector and there by routing table is formed. Each entry in the routing table stores sequence numbers which are even if a link exists; else, an odd number is used. The number is generated by the destination and the emitter requires sending out the next update with this number.

V. PROBLEMS WITH AD-HOC ROUTING PROTOCOLS DUE TO ATTACKS

In ad-hoc routing protocols, nodes exchange information about the network topology with each other, because the nodes are also act as a routers. This fact is also an important atony because a conciliated node could give bad information to redirect traffic or just stop it. Moreover, we can say that security of routing protocols is very destructible. The aim of this part is to provide a description of the causes of the problems with ad-hoc routing protocols.

A. Infrastructure of ad-hoc networks:

Ad-hoc networks have no predetermined fixed infrastructure, that's why the nodes themselves have to deal with the routing of packets. Each node depends on the other neighbouring nodes to route packets for them.

B. Dynamic topology of ad-hoc networks:

The organization of the nodes may change because of the mobility-aspect of ad-hoc networks: they contain nodes that may repeatedly change their locations. Due to this fact, we talk about the dynamic topology of these networks. Dynamic topology is a main characteristic that causes problems: when several ad-hoc networks combine together, there can be transcript of IP addresses, and resolving it is not so easy. Then, attacks can readily occur by using this transcript of IP address (cf. attacks using impersonation).

C. Problems involved with wireless communication:

Routing related control messages can be tampered because of wireless channels have a poor protection to noise and signal interferences. A malicious intruder can just spy on the line, jam, interrupt or subvert the information circulating within this network.

D. Inherent trust relationship between neighbours:

Actual ad-hoc routing protocols assume that all participants are frank. Then, this directly allows malicious nodes to serve and try to palsy the whole network, just by supplying wrong information.

VI. ROUTING PROTOCOL ATTACKS

Ad-hoc networks are more easily attacked than wired network due to their particular architecture. We can categorize into two kinds of attack: the passive attacks and the active attacks. A passive attack does not break the operation of the protocol, but tries to retrace valuable information by listening to traffic. Instead, an active attack injects packets randomly and tries to violation the operation of the protocol in order to limit availability, avail authentication, or attract packets destined to other nodes.

The routing protocols in MANET are quite insecure because attackers can easily obtain information about network topology. Indeed in AODV and DSR routing protocols, the route discovery packets are carried in clear text. So a malicious node can discover the network structure just by analysing this kind of packets and may be able to determine the role of each node in the network. With all these information more grave attacks can be performed in order to disturb the network operation by isolate important nodes, etc. Let us see the different attacks possible by using modification first, then by using impersonation and finally the attacks using fabrication.

1. Attacks using modification

One of the simplest ways for a malicious node to disturb the good operation of an ad-hoc network is to announce better routes (to reach other nodes or just a specific one) than the other nodes. This type of attack is based on the modification of the metric value for a route or by altering control message fields (Denial Of Service attacks).

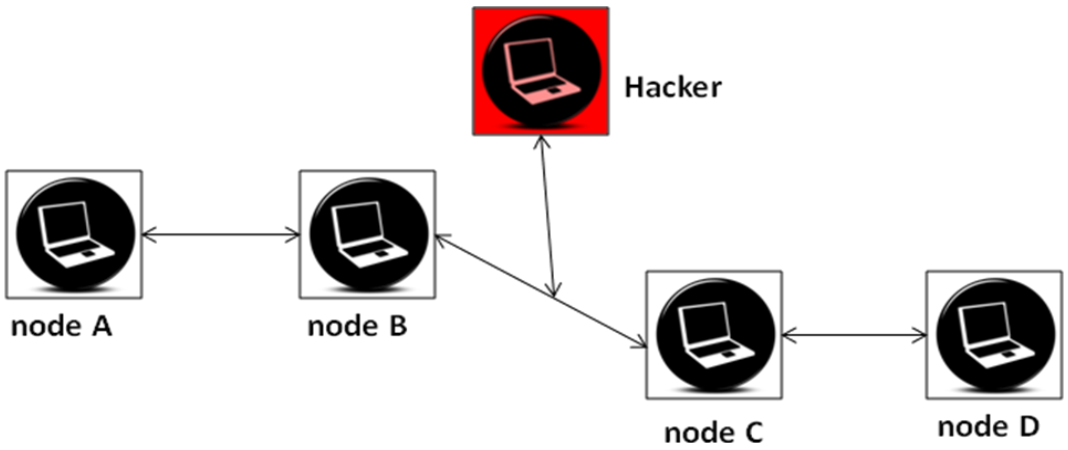

Figure 2

For example, illustrated a network in the Figure 2, a malicious node “Hacker” could keep traffic from reaching the node D by consistently advertising to the node B a shorter route to the node D than the route to D that C is advertising.

A. Redirection by modifying route sequence number

In ad-hoc networks, like in wired networks, the better path is determined by a specific value to reach a destination node, which is the metric and is oft the element, which determines the better route. Smaller this value is better the route. That’s why a simple way to attack a network is to change this value with a smaller number than the last “better” value.

In the figure 2 we have shown that a malicious node called “Hacker” try to insert itself to the network in order to disturb its operation. When the source node A wants to communicate with the destination node D, it broadcasts a message asking all the neighbouring nodes around the better path to reach the node D. Node B will received the message and forward it. The node C will reply that it has a direct route to D and in this reply message; it will give a value for the metric. Now if the malicious node

replies to the node B too that it has a direct route to the node D with a smaller metric value than node C, node B will consider this route as the best one and delete the path by the node C. The result in the example is shown in the figure 3 below.

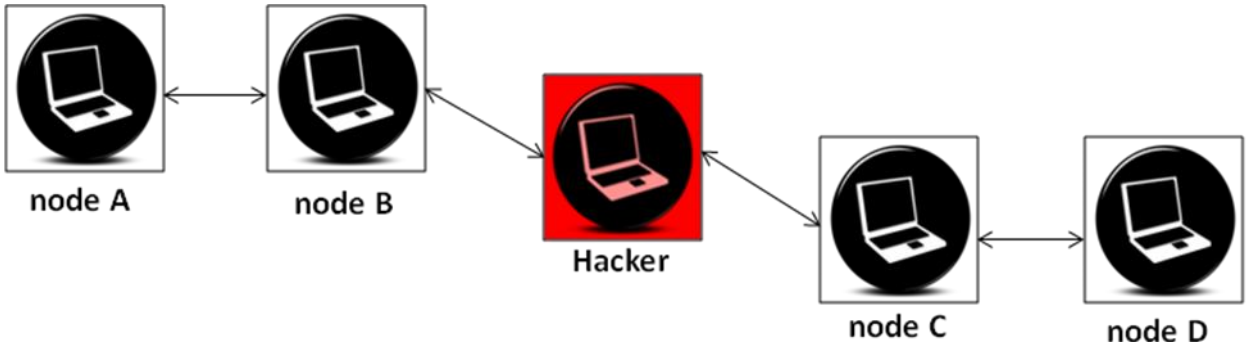

Figure 3

B. Redirection by modifying hop count

When a node cannot decide what the best route is regarding to different metrics, it can use the number of hops to decide which path is the best route to reach a specific node. This is the case in the AODV protocol. In this case, the protocol is determined the best route using the hop count value. Also a malicious node can interrupt the network too, by announcing a smallest hop count value to reach the node. In general, hackers use the value zero to be sure to have the smallest hop count value.

C. Denial of Service (DOS) attacks with modified source routes

The DOS attack is well-known in computer security and can be efficient in ad-hoc networks without secure routing protocols. An easy way to understand the operation of DOS attacks is to see the figure 4. In this figure, a malicious node is located in the network. If the node A wants to communicate with the destination node E, it sends data packets by following its route cache to the node E including the malicious node. The malicious node will also receive the data packets; it can change the header of these packets in order to abort the transmission of the data.

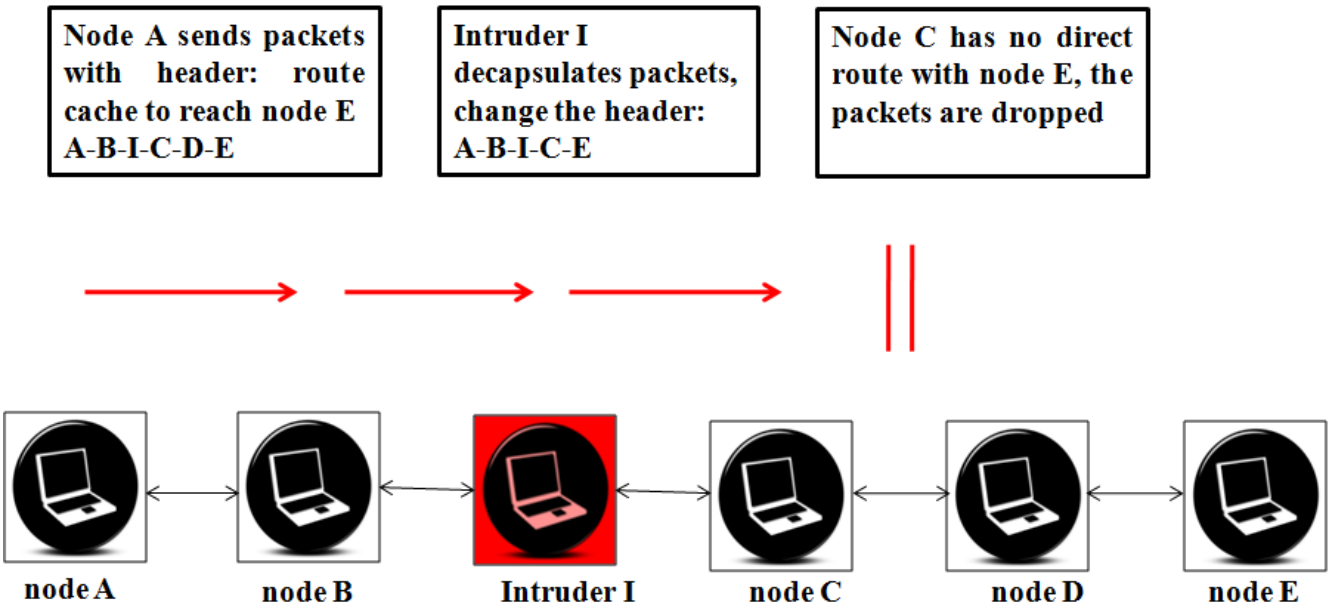

Figure 4

2. Attacks using impersonation

These attacks are called spoofing since the malicious node hide its real IP address or MAC address and uses another one. As a current ad-hoc routing protocols like AODV and DSR do not authenticate source IP address, many spoofing attacks are launch by a malicious node. For example, in the network a hacker can create loops to isolate a node from the remainder of the network. The hacker just has to take IP address of other node in the network and then use them to declare new route (with smallest metric) to the others nodes. By doing this, he can simply modify the network topology as he wants.

3. Attacks using fabrication

Attacks using fabrication can be classified into three types. They are described below:

A. Falsifying route error messages

The first attack is quite common in AODV and DSR because these two protocols are using path maintenance to recover the good path when some nodes have moved. The weakness of this architecture is that when a node moves, the closest node sends an "error" message to the others to inform them that the route is no more available. If the identity of another node arrogates by a malicious node using spoofing and send error messages to the others, the other nodes will modify their routing tables with this updated information. Also the malicious node may insulate any node quite easily.

B. Corrupting routing state:

The promiscuous mode of updating routing table which is employed by DSR, this is a passive attack that can occur in DSR. When information stored in routing table at routers is deleted, updated or injected with false information then this kind of attack occurs. Indeed, in summation to learning routes from headers of packets, which a node is processing along a path, routes in DSR may also be savant from promiscuously received packets. The node is not on the path from source to destination but node overhearing any packet may add the routing information implied in that packet's header to its own route cache.

The vulnerability of this system is that an attacker could easily exploit this method of learning routes and poison route caches. For example, the hacker just has to broadcast a message with a spoofed IP address in the other nodes around. When they will receive this message, the nodes would add this recent route to their cache and also communicate now with this route to reach a special node (the malicious node in fact instead of the one with the same IP address as the hacker's node).

C. Routing table overflow attack

If the ad-hoc network is using a "proactive" protocol, it means that the protocol algorithm try to find routing information even before they are needed. (Instead of "reactive" protocol which do this after). The attacker attempts to create route to non-existent nodes for a vulnerability used by this attack. If he creates enough routes, new routes cannot be created anymore because of an overwhelming pressure of the protocol.

D. Other attacks using fabrication

Replay attack: An attacker sends old advertisements to a node causing it to update its routing table with old routes.
*Black hole***:** An attacker declares a zero metric for all destinations causing all nodes throughout it to route packets towards it.

VII. SOLUTION TO SECURE ROUTING PROTOCOLS

In order to provide solutions to the security issues involved we must first establish that there are different kinds of ad-hoc networks and the different types of networks put different demands on the infrastructure and also determines what means are available to improve security. In ad-hoc networks are classified into the following types:

• Open

The Open environment is characterized by the lack of any infrastructure that one can use in order to maintain security. The nodes ready-for-service in an open environment can be of any type and not necessarily known beforehand. Therefore any kind of central authority system that requires prior knowledge of the nodes in the network is not going to work. Typically this is not a very common environment and the extreme openness it presumes also limits the available security measures a great deal.

• Managed-Open

The managed-open environment is probably the one where most research is being done today as it is the type of environment we are most likely to see expand in the nearest future .In this type of environment there the possibility to use already established infrastructure to some extent to help us secure the ad-hoc network. This opens up a whole new range of strategies using certificate servers and other similar software to provide a starting point of the security in the network.

• *Managed-Hostile*

This is perhaps the classic ad-hoc environment and it's described as nodes in a military war-zone, or probably in a disaster area. Here security is the primary goal and even information such as the location of the nodes involved is considered very sensitive information. In this type of environment security is considered to be much more important than performance and as such the security measures can be made a bit more extreme.

Depending on the type of network environment, different types of security-enhancing techniques have been developed, each of which offers to minimize the security risks while still keeping within the bounds set up by the particular environment. There are two main different approaches to designing the techniques: adding enhancements to existing protocols and creating new protocols from the ground up. They are described below:

1. Protocol enhancements

These techniques are basically enhanced that, if not mentioned otherwise, can be applied to any of the current ad-hoc routing protocols in use today.

A. Security-Aware ad hoc Routing (SAR)

SAR is an attempt to use traditional shared symmetric key encryption in order to provide a higher level of security in ad-hoc networks. SAR can basically extend any of the current ad hoc routing protocols without any major issues. While current ad hoc routing protocols are successful at finding the shortest path to any node within the network, SAR fill this function by finding the shortest path provision a requested trust level. The use of shared symmetric keys for implemented of different trust levels. In order for a node to forward or receive a packet it needs the required key to decrypt it. Any nodes that not on the requested trust level will not have the key and cannot forward or read the packets.

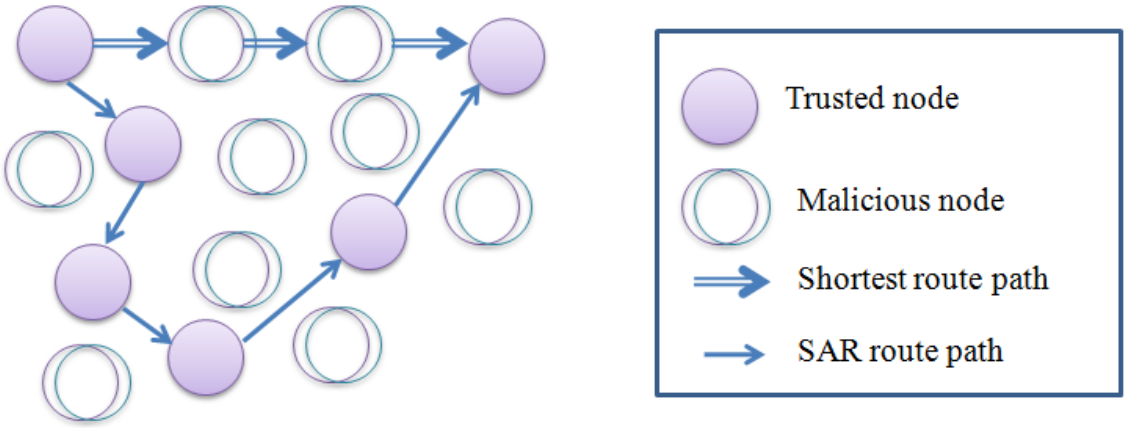

Figure 5

Figure 5 illustrates the difference in route path selection between SAR and a normal ad-hoc routing protocol choosing the shortest routing path. The arrows represent route hops. Every node sending a packet decides what trust level to use for the transfer and thereby decides the trust level required by every node that will forward the packet to its final destination.
SAR is indeed secure in the way that it does ensure that only nodes having the required trust level will read and reroute the packets being sent. Unfortunately, SAR yet leaves a lot of security issues uncovered and still open for attacks:
• Nothing is done to prevent misbehaving (and thereby possibly malicious) nodes from being used for routing, till they have the required key
• If a malicious node somehow rescues the required key the protocol is still open for all kinds of attacks described previously

There is one other main drawback to using SAR and that is the excessive encrypting and decrypting required at each hop, because we are treat with mobile environments the extra processing leading to increased power consumption can be a problem, depending on the kind of mobile devices being used.
SAR is intentional for the managed-open environment as it requires some sort of key distribution system in order to distribute the trust level keys to the correct devices.

B. Secure Routing Protocol, SRP

Secure Routing Protocol (SRP), is another protocol extent that can be applied to any of the most commonly used protocols today. The basic idea of Secure Routing Protocol is to set up a security association (SA) between the source and the destination node. The SA is usually set up by negotiating a shared key based on the other party's public key, and after that the key can be used to encrypt and decrypt the messages. The routing path is always sent along with the packets, unencrypted though (since

none of the intermediate nodes have knowledge of the shared key), thus sharing network infrastructure information to probable attackers. In fact one of the prime security issue that it has no defence against the "invisible node" attack in SRP that simply puts itself (and possibly a large number of other invisible nodes) anywhere along the message path without adding itself to the path, thereby causing potentially large problems as far as routing goes.

C. The Selfish Node

The selfish node is based on one of Darwin's theories of evolution within birds, where birds are divided into suckers (always helping others), cheats (never helping, always receiving help) and grudgers (help those that help them). The theory states that eventually the suckers die first, and then the cheats (since the grudgers won't help them) and the grudgers will reign. This conviction is moved to the open environment ad hoc networks in order to help avoid maliciously behaving nodes.

The open environment poses quite a few new threats to ad-hoc networks. Among others, it is very difficult to recognize a malicious node using certificates since the idea of this kind of environment is that different devices, presumably from very different locations and owners, collaborate to create a functioning network. Since the main goal of such a network is high throughput the simplest and therefore most probable form of attack targeting the main goal is a DOS-attack, and this is what they're trying to intercept.

Using suitably sized cost and profit to routing and forwarding the goal is to more or less isolate misbehaving (possibly malicious) nodes. The following components are used in order to try and keep network throughput at a maximum:

• *The Monitor*

This component acts as a sort of a "neighbourhood-watch", where nodes try to detect bad behaviour in nodes in their vicinity. Bad behaviour that can be detected unusually high routing traffic, unnecessary manifold routing updates flooding and more. Of course, proper thresholds must be used in order for this to work. When harm behaviour is detected an alarm signal is sent to the reputation system.

• *The Reputation System*

This is basically a rating of nodes and what their reputation is. Depending on reported alarms and alarms experienced by the node itself different nodes are rated differently. This component can also use a rumour spreading system to inform other nodes of bad behaving nodes reputation. This way a malicious node will speedily become "notorious" among the other nodes.

• *The Path Manager*

The appropriate changes in routing tables as alarms and reputations changes in the system are taken by the path manager, deletion of malicious behaving nodes from routing tables for instance.

• *The Trust Manager*

The trust manager maintains a list of nodes and how much they are trusted. When an alarm is received depending on how trustworthy the reporting node is, different actions can be taken, since we surely don't want to leave ourselves open for attacks where malicious nodes tries to ban other nodes by sending false alarms.

Each of these components exists within each node and they all help to keep the network alive. The result is a network that in a sense learns that some of the nodes are malicious and therefore isolate them. Indeed this is a very different approach then the other mentioned systems but keep in mind that this is the only one really intended for the open environment, with nodes of unknown origin cooperating to achieve maximum network throughput. That is why it is focused on different kinds of DOS attacks and not concentrating on encrypting traffic and such. Also note that in the open environment no use of existing infrastructure is to be used, which leaves the previously mentioned systems useless since they more or less all require existing infrastructure (i.e. certificate servers).

2. Secure protocols

These are protocols designed from the ground up to provide ad-hoc networks with all the required features described earlier.

*A. Authenticated Routing for Ad-hoc Networks (ARAN***)**

ARAN is a protocol designed to provide secure communications in managed-open environments. Like SAR it makes use of present infrastructure in the form of certificate servers. The protocol has two phases, authentication and transmission.

a. Authentication

The goal of the first phase is to make sure that a secure path from the source node A and the destination node B can be established. The phase requires that each node has received a certificate from a trusted certificate server. The certificate contains a node's IP number, public key as well as the time of issuing and expiration.

Node A broadcasts a signed (using A's key) route discovery packet (RDP) to all its neighbouring nodes in order to find a route to B. Each node that gains the RDP for the first time removes any other intermediate(not A) node's signature, signs the RDP that dealing with its own key and broadcasts it to all its neighbouring nodes, saving a route pair (A,B) in its routing table. This continues until node B lastly receives the packet. Node B then sends a reply packet containing its own certificate and signed using its key, the packet is sent along the reverse path (each intermediate node sends it back to where the original RDP came from). When A gets the REP packet, it checks that the signature is correct and stores node B's certificate to use in the next phase.

The procedure does ensure loop freedom as well as makes sure that B really is B using the certificates (providing of course that the certificate server has not been compromised). One of the downsides to this procedure is that each node has to store the source-destination routing pairs instead of just routing based on destination which is used in other protocols.

b. Transmission

A now needs to discover the shortest path to B and therefore sends a "Shortest Path Confirmation (SPC)" packet to all its neighbours, encrypted using B's public key. Each successive intermediate node encrypts the message again using B's public key and including its own certificate then forward it to its neighbours. When B eventually receives the SPC packet it checks all of the signatures and replies to the first SPC received, as well as all other SPCs having a shorter recorded path (the path is recorded in the encrypted keys). B then sends a "Recorded Shortest Path (RSP)", packet back to A, including the path to use in the packet. A can nicely verify that it comes from B and that it equal to the original SPC sent. This way A has a shortest, secure path to B to transmit data over.

Since at all forwarding the packet is re-encrypted using B's public key, only B is able to discover the actual route taken. This way spoofing attacks or other attempts to misdirect the packets will fail since the malicious nodes first would have to crack the encryption. Only using B's private key would that be possible. Hence, the so called "invisible node-attack" is also prevented using this protocol.

One of the main issues using ARAN is the required certificate server, which means that the integrity of that server is vital. This is by design though and as it is intentional for a managed-open environment it shouldn't be considered a big issue.

B. Secure Position Aided Ad hoc Routing (SPAAR)

The Secure Position Aided Ad hoc Routing (SPAAR), protocol was developed with the classical managed-hostile environment in mind, thus meant to provide a very high level of security, occasionally at the cost of performance. Among other things, SPAAR also requires that each device use a GPS locator to determine its position, although some leeway is given to nodes using a so-called "locator-proxy" if absolute security is not required.

The certificate system is similar to ARAN in that a combination of a public key and the public key of the certificate server is used, although in SPAAR a third key is also generated, a group neighbourhood key that is used to decrypt Route Request packets, RREQ. The invisible node-attack is to avoid in SPAAR packets are only accepted between neighbouring nodes one hop away from each other. Saving certificate nodes also use the location of the other nodes when attempting to communicate, a maximum distance N is set that decides how far away a node can be and still be called a neighbour.

The basic transmission procedure is quite similar to ARAN, although the group neighbourhood key is used for encryption in order to ensure one-hop communication only. Since all nodes also have information on their location they only forward RREQs if their position is closer to the destination position. The source node needs to know the approximate location of the destination in order for the routing to be efficient because destination node reply the location and velocity-vector of the destination.

SPAAR may seem a bit rearward, using multiple keys and GPS location-dependent routing. Considering the nature of the managed-hostile environment this is not very strange. In the situations this environment presents, finding the geographically shortest path can be at least as important as finding the fastest path, whether its in a battle field or a disaster area. Also, it discloses no information on the network layout to any non-authorized nodes, something which also can be essential when relay stations are secret.

The only real security problem currently discovered in SPAAR is once again the usage of the certificate server and the extreme need to keep this server uncompromised. Also, issues stably exist with compromised nodes already having valid certificates.

VIII. CONCLUSION

We conclude that the mobile Ad-hoc networks are prone to various kinds of vulnerable attacks, however besides all these hazards there are plenty of security routing protocols available which make them more secure and error-free networks, therefore fulfilling the ultimate aim of Ad-hoc networks i.e. the accomplishment of instant network regardless of the types of nodes or type of prevailing environments.

REFERENCES

[1] "*Review Paper on Detection and Prevention Techniques of Gray-Hole Attack in Manet*" A. Desai International Journal of Computer Science and Mobile Computing Vol. 2, pp. 105-108, May 2013.
[2] "A Survey on Detection and Prevention Techniques for Gray-Hole Attack in MANET" M.K. Kumawat, J.S. Yadav (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 1288-1290.
[2] "*Intrusion Detection in Wireless Ad-hoc Networks"*, Yongguang Zhang, Wenke Lee, 2000, http://www.wins.hrl.com/people/ygz/papers/mobicom00.pdf
[3] "*Securing Ad-hoc Networks"*, L. Zhou, Z.J.Haas, 1999, Cornell University, http://www.cs.cornell.edu/home/ldzhou/adhoc.pdf
[4] *"A Secure Routing Protocol for Ad Hoc Networks"*, Bridget Dahill, Brian Neil, Elizabeth Royer, Clay Shields, 2000, http://www.cs.umn.edu/research/mobile/seminar/SUMMER03/WNfiles/aran.icnp02.pdf
[5] *"Security-Aware Ad-Hoc Routing for Wireless Networks"*, Seung Yi, Prasad Naldurg, Robin Kravets, 2001, University of Illinois, http://www-old.cs.uiuc.edu/Dienst/Repository/2.0/Body/ncstrl.uiuc_cs/UIUCDCS-R-2001-2241/pdf
[6] "*Mitigating Routing Misbehaviour in Ad Hoc Networks"*, S. Marti, T.J. Giuli, K Lai and M. Baker, 2000, Stanford University, http://mosquitonet.stanford.edu/~laik/projects/adhoc/mitigating.pdf
[7] "*Security in Ad-Hoc Routing Protocols"*, Deshpande Vivek S., Lecturer, Maharashtra Institute Of Technology Women Engineering Pune, Maharashtra, India.

