Study and Analysis on Security of Ad-Hoc Networks

KDRS Kuruppu[#] and TL Weerawardane

Department of Electrical, Electronic and Telecommunication Engineering
General Sir John Kotelawala Defence University
Rathmalana
Sri Lanka.

[#]rsachira@live.com

Abstract— *Mobile Ad Hoc Network (MANET) represents a system of wireless mobile nodes that can freely and dynamically self-organize into arbitrary and temporary network topologies. Due to this dynamic nature and due to the absence of centralized infrastructure MANETs are more susceptible to attacks. Furthermore, due to these characteristics typical security systems and techniques cannot be employed in MANETs. Furthermore, since MANET's nodes are mobile, they are power limited and computationally limited. Therefore, traditional security schemes which are computationally expensive and require more power are not feasible to be implemented in MANETs. As a result, to protect MANETs against its vulnerabilities, systems and techniques have been specially developed to suit its conditions. This study analyses the vulnerabilities of MANETs and describes various protection schemes that had been developed to overcome those. Moreover, this study analyses shortcoming and vulnerabilities of those protection schemes and finally present areas which require further research and development.*

Keywords— **MANET, Ad Hoc, networks, security, routing**

I. Introduction

Ad Hoc network is a collection of autonomous nodes that form a dynamic, purpose-specific, multi-hop radio network in a decentralized fashion (Li and Joshi, n.d.). The quintessential nature of Ad Hoc networks is the absence of fixed support infrastructure such as mobile switching centers, base stations, access points, and other centralized devices seen in typical wireless networks. The network topology of such networks is dynamic. Nodes join and leave as they please. Furthermore, due to ever-changing network topology and unavailability of centralized structures, network operations such as packet forwarding, routing etc. are carried out by individual nodes. Ad Hoc networks are referred to as Mobile Ad Hoc Networks (MANET) due to this inherent mobile nature.

MANETs have various uses in different scales. They can be classified into four main classes based on the coverage area: Body, Personal, Local and Wide Area Networks (Conti, 2003). Body Area Network (BAN) is strongly correlated with wearable computers distributed on the body eg: head-mounted displays, microphones, earphones etc. The communication range of BAN is about 1-2 meters i.e. body range. Personal Area Network (PAN) connects mobile devices carried by users to other mobile and stationary devices. PAN has a communicating range of upto 10 meters (Conti, 2003). PAN MANETs are usually used to share internet connections between computers and mobile devices. Local and Wide MANETs have a communicating range of 100-500 meters and unlike normal LAN and WAN do not have centralized controllers or Access Points.

Although MANETs can have many applications, MANETs are avoided in commercial applications since they are inherently unsecure. Dynamic behavior of nodes and lack of centralized infrastructure prevents typical security schemes from being implemented in MANETs. Due to this MANETs are more vulnerable than other wireless networks.

Vulnerabilities of MANETs have been analyzed in security surveys such as (Li and Joshi, n.d.). Moreover, (Li and Joshi, n.d.) describes some protection mechanisms such as intrusion detection systems etc. Shortcoming of such analysis studies are that most of these studies describes old methods. There are some new methods such as Adaptive intrusion detection systems based on neural networks, which have not been addressed by these papers. Furthermore, most of these papers only provide a description of the protection methods. They do not describe actual implementations and actual operation of these methods. And most of the survey papers do not analyze the vulnerabilities in these protection methods. This study attempts to overcome those shortcomings and attempt to provide a much more descriptive picture of the current state in MANETs. Moreover, this paper attempts to help researchers to pick a field of study by identifying the current issues with MANETs.

This study describes the vulnerabilities of MANETs and analyzes security systems and techniques used to overcome those vulnerabilities. Furthermore, this study identifies weaknesses in various protection methods that can be exploited by an attacker. Finally, in the conclusion, it summarizes the security problems in MANETs and in various protection methods and identifies potential research areas relating to MANETs.

II. Classification of Attacks in Ad Hoc Networks

Attacks in Ad Hoc networks can be mainly classified into two types (Khatri, Bhadoria and Narwariya, 2009): a) External attacks, b) Internal attacks. External attacks are carried out by adversaries, which are in the proximity but are not trusted nodes of the network. An external attacker may cause congestion, propagate fake routing information and try to disturb nodes from providing services. These attacks are similar to the normal attacks in traditional wired or wireless networks. Therefore, this type of attacks can be prevented and detected using conventional security methods such as membership authentication or firewall (Khatri, Bhadoria and Narwariya, 2009).

'Internal attacks' are carry out by nodes within the network. Due to the pervasive nature of communication in Ad Hoc networks, and due to the open nature and absence of centralized bodies, these type of attacks are far more dangerous for Ad Hoc networks than its counterpart.

Furthermore, attacks can be classified as a) Passive attacks and b) Active attacks (Li and Joshi, n.d.). Passive attacks typically involve eavesdropping without trying to change the behavior of protocols. Convert Channels, traffic analysis, sniffing to compromise keys can be classified as passive attacks. Active attacks are ones in which the attacker try to change the behavior of the network by replicating, modifying, deleting exchange data. An adversary may use a combination of active and passive attacks where, information inadvertently disclosed to passive attackers by the protocol packets are used to launch active attacks.

It can also be seen that attacks on Ad Hoc networks can be classified according to the level (Khatri, Bhadoria and Narwariya, 2009): a) Attacks on basic mechanism of the network such as routing, b) Attacks on security mechanisms and notably on key management mechanism.

Some malicious behavior that exploit weaknesses in ad hoc networks, which falls under Internal attacks may be attacks i.e. offensive movements carried out to sabotage the network, however it can also be selfishness of a node/nodes in order to preserve battery life etc. Therefore, malicious behavior by nodes can be classified as a) Attacks and b) Selfishness.

III. Attacks on MANETs

A. Denial of Service Attacks (DoS)

Denial of service attacks is aimed to crab the availability of certain node or even services of the entire ad hoc network (Djenouri, Khelladi and Badache, 2005). DoS attacks can be either internal or external. DoS that fall under Internal attacks can be due to offensive movement i.e. attacks by adversaries or it can be due to selfish behavior of a node/nodes (eg: not performing the service in order to save battery life).

DoS attacks in typical wireless networks are carry out by flooding a centralized system that provides a service with network traffic so as to exhaust its processing power. However, ad hoc networks are immune to this kind of DoS attacks due to its inherently decentralized nature. That is because services are carried out collaboratively. Even if one node fails, the other nodes will provide the service.

However, MANETs are more susceptible to DoS attacks due to interference prone radio channels and limited battery power. Attackers can use radio jamming to conduct DoS in traditional wireless area networks and in MANETs. Additionally, attackers can also use battery exhaustion methods to perform DoS in MANETs because unlike in WAN nodes in MANETs are mostly battery powered due to their mobile nature.

DoS attacks can be conducted as both Internal Attacks and External Attacks. However, all DoS attacks are active attacks. DoS attacks are usually conducted on basic mechanisms of the network such as routing. In fact, most DoS attacks are conducted in the physical layer (jamming) and by exploiting weaknesses in routing protocols. However, they can also exploit security mechanisms as well.

To perform a DoS attack, an attacker must first identify the most important nodes in the network since performing the attack on a node that is not used by others will not affect the network. An attacker can passively eavesdrop on the routing packets to determine important nodes in the network. If a route to a node is requested more often, then the attacker can safely assume that, that node is important to the network. He may then target that node with DoS attacks to sabotage the network.

There are many ways to perform DoS attacks. One of the popular ways is by using routing. An attacker may overwhelm network traffic to a targeted node by sending it routing packets to be forwarded or he can confuse the node by sendifng wrong/contradicting routing packets. Attacker (an internal attacker) can either generate routing packets or, he can replicate and replay routing packets it had received. This way the attacker can either overwhelm the target or confuse it so as to sabotage its services.

DoS attacks can also be performed by exploiting weaknesses in the security mechanisms. Most of the time these methods are used to disrupt services of intrusion detection systems. An internal attacker can overwhelm IDS agents or other nodes in the path of IDS agents by repeatedly requesting intrusion detection state information from their cooperative detection engines. Another popular method is poisoning. Poisoning is used on isolated IDSs. In this method, the attacker sends false alarms to the IDS trying to put the IDS out of service.

B. Impersonation

Impersonation attack is a severe threat to the security of mobile ad hoc network (Djenouri, Khelladi and Badache, 2005). It is difficult to implement authentication systems in MANETs due to lack of centralized structures and due to its inherently mobile nature. If a proper authentication mechanism is not implemented, an attacker will be able to join the network undetectably sending false routing information and will be able to masquerade as some other trusted node (Li and Joshi, n.d.). Impersonation attacks are all active attacks as they usually involve modification and replication of packets. It is difficult for an external node to impersonate a node within the network due to firewalls. This is impossible in a reasonably secured MANET. There is much more chance of an internal attacker impersonating another node. Impersonation attacks are a security risk at all levels. Within network management, the attacker could gain access to configuration system as a superuser. At the service level, an attacker could have its public key certified without proper credentials (Li and Joshi, n.d.).

However, these types of attacks are likely to be noticed very quickly. Therefore, the information that is manipulated and accessed is not crucial enough to make the attack worthwhile. Furthermore, current MANETs have authentication mechanisms, which enable a node to trust the origin of data it has received. This mitigates impersonations.

Authentication is realized by applying digital signatures or keyed fingerprints in all layers eg: over routing messages, configuration or status information, exchange payload data etc.

An issue faced by MANETs is that Digital signatures that use public-key cryptography are problematic to implement in MANETs due to the relatively high computational power involved and since this technique requires an efficient and secure key management service which is difficult to realize without centralized structures. In many cases lighter solutions such as keyed hash functions or a priori negotiated and certified keys and session identifiers are used (Li and Joshi, n.d.). This however does not provide the same protection or confidentiality offered by public key cryptography.

C. Eavesdropping

Eavesdropping is one of the most common passive attacks. The goal of eavesdropping is to obtain confidential information by a node to which it is not entitled. Eavesdropping can occur as external attacks where an external node in the vicinity tries to eavesdrop on the network or as internal attacks where a node tries to acquire data to which it is not authorized.

Although it may be difficult to spoof, an attacker can easily gather background information of the network. Usually most MANET routers are not suitable to support IP protection mechanisms due to limited resources (limited resources of MANET routers to support IPsec stack) (Treesa, 2013). In such cases it is relatively easy for an attacker to gain topological information of the network by using a malicious NHDP router. It may also eavesdrop on data traffic to learn sources and destination addresses of data packets, or other header information. Even though this does not pose a direct threat to the network nor to NHDP, information gathered can be used for other attacks such as DoS.

Therefore, it is required to make lightweight IP security mechanisms that are not very resource intensive to be implemented in MANETs.

D. Trust Attacks

Trust hierarchy is a representation of privilege levels, which reflects the security, importance of each node. Trust attacks can be considered as impersonation attacks where the attacker tries to gain access to a service or data by identifying itself as belonging to a certain trust level, which in reality it does not have. Routing protocol packets in existing MANET algorithms does not carry authentication identities (Li and Joshi, n.d.). This is a major loophole for trust attacks. Techniques such as ‘Secure transient associations’ and ‘Tamper resistant nodes’ are used to counter trust attacks.

IV. Attacks against Routing

Attacks against Routing can be categorized as internal and external attacks. ‘External attacks’ are carried out by attackers outside the network while ‘Internal attacks’ are carried out by attackers inside the network (who are members of the network). Jamming a popular external which can be considered as an attack against routing although it affects data transfer as well. External attacks are not addressed in attacks against routing since those are attacks on the physical layer and therefore cannot be addressed using routing algorithms and intrusion detection algorithms.

Internal Attacks against Routing are much more popular than external attacks. There are numerous types of Internal Attacks are against routing, and are more commonly used than any other kinds of attacks.

This section discusses about vulnerabilities of AODV (Ad hoc On Demand Distance Vector routing protocol). On demand routing protocols only initiate a route discovery process when needed. When an originating node wants to send data packets to a destination but does not have a fresh enough route in its routing table it broadcasts a RREQ (Route REQuest) message to its neighbors (Yi, 2015). AODV uses RREQ to request a path to a destination and to update the path from nodes to originator. And RREP messages to notify about a path to destination to the originator and other nodes (Yi, 2015). Nodes only accept the most recent RREQ, this is guaranteed by RREQ ID. The ID indicates how fresh the request is, higher the ID the better.

Table I summarizes issues with various routing protocols in MANETs.

TABLE I. Security Issues with Routing Protocols in MANETs

Protocol	Security Negatives
OSPF	Age field not protected by digital signature; Area Border Routers and Autonomous System Boundary Routers can generate false routing information.
S-AODV	High overhead; possible route discovery corruption; Compromise of IP portion.
SMT	Limited protection against compromised topological information.
DDM	No access control (needed for group membership restriction).
OLSR	No guarantee in very dynamic environments.
ODMRP	No security means.
AODV	No security means.
TBRPF	No specific mechanisms for security.
SRP	Possible attack when nodes collude during the two phases of a single route discovery.

Secured routing mechanisms such as ARAN, Ariadne, SEAD have been developed to overcome the shortcomings of AODV, however these are preventive approaches that rely on cryptography to ensure the security of the network (Perkins, Belding-Royer and Das, 2003). Therefore, these mechanisms are not effective against attacks from insiders who have access to keying materials.

We can identify several goals an attacker would want to achieve by manipulating the routing layer. They are: (1) Route Disruption: breakdown a route or prevent a route from being established. (2) Route Invasion: attempt to add an attacker into a route between two communication nodes. (3) Node Isolation: prevent a node form communicating with any other nodes. (4) Resource consumption: Consume communication bandwidth of the network. Furthermore, we can identify 3 most basic actions an attacker can perform individually or combined in order to form an attack on the network. (1) Dropping of RREQ messages (RREQ_DR), (2) Modification of RREQ messages (RREQ_MF), (3) Generation of fake RREQ messages (RREQ_AF). Table II specifies whether a given goal can be achieved by a given action.

TABLE II. Utilization of Various Actions in Attacks

Action	Route Disruption	Route Invasion	Node Isolation	Resource consumption
RREQ_DR	Yes	No	No	No
RREQ_MF	Yes	Yes	Partial	Yes
RREQ_AF	Yes	Yes	Partial	Yes

A. *Black-Hole Routers*

This is a DoS attack where a malicious node claims to have the shortest route to a destination through it, but refrains from forwarding packages it receives to the destination (Hu, Johnson and Perrig, 2002). This is achieved through route invasion. The attacker invades the route between its target and other nodes by using RREQ_MF or RREQ_AF, it can then drop the packages it receives and cause a DoS attack.

B. *Grey Hole Routers*

This is a small variation of Black hole routers. In this attack, the attacker does not drop all the packages like in the black hole attack. Dropping all packets can cause the source to find new routes reducing the time of attack. And Intruder Detection Systems (IDS) like pathrater will easily be able to identify the attacker. Therefore, in this method the attacker selectively drops packages. This method does not deny the all services but hinder the performance. This attack is harder to identify because this reduction of network capabilities could be produced by the normal instability from wireless connections.

C. *Resource Exhaustion*

Resource exhaustion can cause by two methods. The attacker can flood the network with routing messages (RREQ) using RREQ_AF or RREQ_MF by replicating and replaying RREQs. The attacker can also try to create routing loops by RREQ_MF in order to exhaust resources. Resource exhaustion attacks can also be considered as DoS attack.

D. *Man-in-the-middle*

In this method, the attacker claims to have the shortest path to all or most of nodes and directs all the packages it gets through the victim in order to overwhelm the victim. The attacker uses route invasion discussed above to invade the paths between nodes and their destinations. The attacker would use RREQ_MF or RREQ_AF to achieve this. Once it manages to invade all the routes, it can direct all that traffic through its victim.

E. Wormhole Attacks

The wormhole attack is one of the most sophisticated and serious threats against MANET routing, comprises a pair of attackers. These two attackers act in collusion to record packets at a particular location in the MANET topology and replay them at another node by using a high-speed private network. Wormhole attacks can be used to show a victim that the closest path is through the attacker. Therefore, this attack can be used before Black-Hole attacks, Grey hole attacks and man in the middle attacks to capture the path.

V. Key Management in MANETs

Key management is a major area of interest in MANETs. Some of the attacks mentioned above such as eavesdropping can be mitigated using a decent key management system. Furthermore, key management systems can be used to develop trust levels, authentication mechanisms, private communication etc. However, typical key management systems cannot be implemented in MANETs due to its dynamic nature and lack of centralized infrastructure. In this section, some novel key management systems that can be utilized in MANETs are analyzed.

A. Distributed Asynchronous Key Management Service

Implementing the usual public key cryptography is problematic in MANETs due to its involvement of central certification authority. This method enables the utilization of public key cryptography without the need of a central certification authority. In this method, a service has a public/private key pair K/k. The public key 'K' is known to all the nodes in the network. The private key 'k' is divided into n shares s_1, s_2,…s_n and a single share is given to each server. Each server 'i' also has a public/private key pair K_i/k_i and knows all the public keys of all nodes.

To address the dynamic behavior of MANETs nodes, and to ensure discreteness, this method allows to create a signature with the private key 'k', using 'm' out of 'n' (where m < n) servers (each with a part of k) by combine their knowledge. However, combining the shares do not reveal the actual private key, rather generates a signature based on the private key. The correctness of the signature is verified using the public key, which is typical in public/private key schemes. This method is called threshold cryptography i.e. in (n, k) threshold cryptographic scheme private key is shared among n servers, but k can accurately form a signature (k < n).

Fig. 1. explains a (3, 2) threshold cryptography scheme where m is the message, PS(m, s_i) is the partial signature generated using the private key share s_i and $(m)_k$ the generated signature of m.

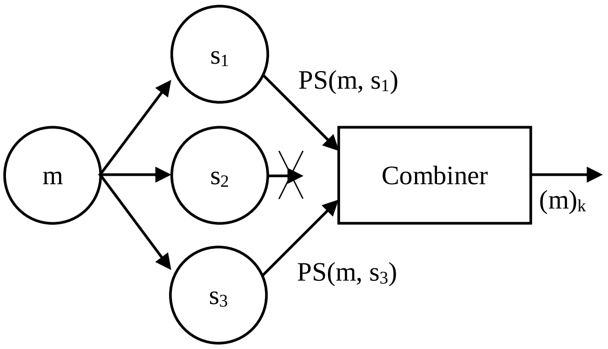

Fig. 1. Signature generation process

B. Progressive Trust Negotiation Scheme

This key based scheme is aimed at building trust between nodes and to mitigate eavesdropping by external as well as internal attackers.

The scheme utilizes a trust model that can be subdivided into two main components: (1) Peer-to-peer component, (2) Remote component. Peer-to-peer component deals with securing communication between neighbors (nodes in radio range) while remote component has the dual responsibility of carrying out trust negotiations and establishing secure end-to-end communication.

Peer-to-peer component requires symmetric encryption keys to be negotiated using Station-to-Station protocol (STS). This prevents external attackers from eavesdropping.

Remote component requires end-to-end key negotiation between communicating nodes. This protects the communication against internal attackers (eavesdroppers). The end-to-end trust negotiation is carried out by incrementally exchanging certificates (peer-to-peer ones). These certificates are used in the remote component's STS key exchange for authentication and thereby to generate a symmetric key between the end points.

Fig. 2. Explains the key formation process. Where (A, B), (B, R), (R, C), (C, D) are neighbors with peer-to peer keys $K_{1,}$ $K_{2,}$ $K_{3,}$ K_4.

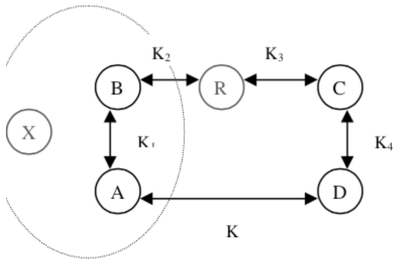

Fig. 2. Key formation process

VI. Intrusion Detection Systems

Due to the security issues in routing systems Intrusion Detection Systems (IDS) have been designed to detect and mitigate these exploitations. This section discusses 5 intruder detection systems.

C. Watchdog

Watchdog is a method by which we can detect misbehaving nodes (Ning and Sun, 2006). When a node forwards a packet, the watchdog checks to see if the next node of the path also forwards the packet (Ning and Sun, 2006). Watchdog maintains a buffer of recently sent packets. It compares each overhead packet with packets in the buffer. If a match is found, that packet is removed. If a packet remains in the buffer for longer than timeout, that packet is considered dropped, and the node responsible is tallied as misbehaving. Once the tally of a particular node exceeds a threshold value that node is determined to be misbehaving, and the source is notified.

Watchdog has some limitations. It is unable to detect misbehaviors in the presence of (1) Ambiguous collisions (2) Receiver collisions (3) Coordinated attacks of two different malicious nodes.

Ambiguous collisions are when some ambiguous problem prevents a node from overhearing transmission of another node. These collisions can occur in such a way disabling the watchdog from overhearing transmission by some node. Therefore, the watchdog has no way of knowing whether that node transmitted the packet or not.

Receiver collision mean, the sender node (the watchdog) can tell whether the next node transmitted the packet, but it cannot tell whether the recipient (next hop) actually received the packet. A malicious node can fool Watchdog by limiting its transmission power so that the recipient does not receive the packet.

Watchdog can only monitor a single node (single hop) at a time, therefore, a group of malicious nodes can carry out coordinated attacks without detection.

A new IDS called Enhanced Adaptive ACKnowledgement (EAACK) had been proposed which addresses all the above mentioned issues including false misbehavior reports.

D. Pathrater

Pathrater is designed to avoid routing packets through misbehaving nodes. In pathrater, each node maintains a rating for every other node it knows about in the network. It calculates a path metric by averaging the node ratings in the path. This rating gives a comparison of the overall reliability of different paths. If there are more than one path, pathrater selects the one with the highest rating i.e. the most reliable path.

One major drawback of pathrater is, although it avoids selecting routes that include unreliable nodes, it does nothing to punish those nodes. These nodes can continue to use network resources and continue their behavior. Such issues have been addressed by novel systems like Confident Intrusion Detection system (Viranda, n.d.).

E. Confident IDS

This technique is similar to watchdog and pathrater. Each node monitors the behaviors of neighbor nodes within its ratio range and learns from them (Viranda, n.d.). However, this technique addresses some of the shortcomings of these two IDSs mentioned above. CONFIDENT IDS comprises of 4 systems. (1) Monitor system, which keep watch on nodes in the communication range. (2) Reputation system, which maintains a rating for each node. If a node does not cooperate it is given a negative rating otherwise a positive rating. (3) Trust manager, which keeps a list of trustworthy nodes. This is used to identify that a message it received is from a trusted source or not. (4) Path manager prepares routes from source to destination excluding paths that contain malicious nodes. Alarm messages are used by trust manager to warn other nodes about unfriendly nodes, in cases where the reputation of a node is debatable. Using the warning system CONFIDENT IDS is able to penalize malicious and selfish nodes by not using them in routing and not forwarding packets through them (Viranda, n.d.).

One key issue in this IDS which is that it does not prevent false reports. It allows negative reports to pass through, which can be exploited by attacker to carryout DoS attacks. Another problem with this technique is, it does not take into account whether a node is acting selfishly due to genuine reasons eg: low battery power. In such a case it will not be fair to penalize such a node.

F. Cluster Based Intrusion Detection Schemes

MANETS have limited power. Therefore, it is not efficient to make each node always a monitoring node. To address this issue Cluster-Based intrusion detection scheme had been introduced. A cluster is a group of nodes that are close to each other. That is, the clusterhead has all its members in 1 hop vicinity. The cluster head of a cluster monitors all the members of that cluster for malicious behavior.

The cluster head is selected via an algorithm, which gives equal chance to all nodes. And is selected for a fixed time.

Cluster-Based IDS are able to get a bigger picture of the situation rather than collaborative IDS, which work, in isolation. As a result, this type of IDS is able to detect poison attacks, which are a major threat to collaborative IDS.

Cluster-Based intrusion detection systems are criticized in some papers. Although this system is ideally able to address the power limitation in MANETs, (Khatri, Bhadoria and

Narwariya, 2009) argues that due to the complexity and number of variables associated with a proper selection process and handovers, this system has the same power usage or even more. Another issue with Cluster-Based IDS is the finite probability of a malicious node being elected. The cluster head is able to perform selfish activities until the re-election timeout expires.

VII. Other Measures to Secure MANETs.

Apart from intrusion detection systems, which are add-ons to MANETs, other measures such are secured routing protocols have been designed to make MANETs more secure.

A. Security-Aware Ad hoc Routing protocol (SAR)

SAR is an on-demand routing protocol based upon conventional routing protocols such as AODV and DSR. SAR was primarily designed to defend against possible Black-Hole attacks.

In SAR some security metrics are embedded in the RREQ apart from the usual information. This ensures that an intermediate/destination node can process the packet or forward it only if it can provide the required security or has the required trust level/authorization. If a node cannot provide the required security, the packet is dropped. As a result, SAR only detect routes with a guarantee of security. It may fail to find a route between two nodes even if they are connected but do not have a route with the required guarantee of security.

SAR tries to build a route comprising of same trust level nodes. Each trust level has a different shared key. Therefore, only same trust level nodes can read RREQs (Sanzgiri et al., 2002). This prevents nodes with higher or lower trust levels from causing interruptions as they are supposed to drop the packets anyway.

This also leads to a major drawback in SAR. A route comprising of higher trust level nodes must be valid. Therefore, avoiding higher trust level nodes is undesirable.

B. SEAD

SEAD is a secure routing protocol based on the DSDV-SQ version of the insecure DSDV ad hoc routing protocol. SEAD employs destination sequence numbers (which are used by DSDV to avoid routing loops) to provide replay protection to routing updates. SEAD does not use the average weighted settling time delay as in DSDV to avoid wormholes.

Shortcomings of SEAD include: routing loops are possible in SEAD if the loop contains one or more attackers; In the current version it cannot detect nodes that advertise routes but do not forward packets.

C. TIARA

Research efforts at Architecture Technology Corporation are aimed at demonstrating a set of innovative design techniques, collectively called TIARA (Techniques for Intrusion-resistant Ad Hoc Routing Algorithms), that strengthen ad hoc networks against denial of service attacks. The TIARA mechanisms limit the damage sustained by ad hoc networks from intrusion attacks and allow for continued network operation at an acceptable level during such attacks (Lidong and Haas, 1999).

D. Grammatical Evolution Approach to Intrusion Detection

This is an intrusion detection system that uses artificial intelligence based learning techniques to explore the design space. This approach is inspired by the natural evolution. It can be used to detect known attacks such as DoS and route disruption attacks. In this method, intrusion detection programs are evolved for each attack and distributed to each node on the network.

Other intrusion detection systems based on artificial intelligence and learning techniques have been developed. These detection systems known as 'Anomaly-based detection' are capable of detecting novel attacks. However, these techniques are still in the development state.

VIII. Conclusion

It can be seen from the above facts that still a clear-cut security scheme has not been designed for MANETs. There are various algorithms and security schemes to overcome different threats, but a system that can deal with all possible threats and vulnerabilities of MANETs will have to be built by optimally combining the available schemes.

It can be also seen that one of the major threats in IDS: a compromised node getting elected as a cluster head is not properly addressed. Therefore, more research must be done on IDS to properly address such issues.

It can be seen that there are still issues with attacker identification. Attacker identification techniques can be improved by making ways to minimize false alarms, and manipulations by compromised nodes.

Furthermore, all IDS techniques treat nodes as equals, but in real applications there can be nodes with special tasks (eg: fire alarms etc.) these must not be classified as selfish nodes/malicious nodes when they do not cooperate with packet forwarding etc. since it is not that nodes main priority.

Furthermore, IDS must give some excuse to nodes with low battery capacity or low power to be selfish up to an extent.

With Internet of Things (IoT) getting popular, ad hoc networks will be widely used in the future. Most of these applications will have devices with low battery capacities and low processing power, therefore much more efficient algorithms for key management, intrusion detection, routing algorithms etc. which require less processing power will have to be built.

REFERENCES

Caballero, E. (2006). Vulnerabilities of intrusion detection systems in mobile ad-hoc networks—the routing problem. *TKK T-110.5290 Seminar on Network Security*.

Conti, M. (2003). Body, personal, and local ad hoc wireless networks.

Djenouri, D., Khelladi, L. and Badache, A. (2005). 'A survey of security issues in mobile ad hoc and sensor networks. *IEEE Commun. Surv. Tutorials*, 7(4), pp.2-28.

Hortelano, J., Cano, J., Calafate, C. and Manzoni, P. (n.d.). Watchdog intrusion detection systems: Are They Feasible in MANETs?.

Hu, Y., Johnson, D. and Perrig, A. (2002). SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks. *Fourth IEEE Workshop on Mobile Computing Systems and Applications*.

Khatri, P., Bhadoria, S. and Narwariya, M. (2009). 'A Survey on Security issues in Mobile ADHOC networks. *TECHNIA – International Journal of Computing Science and Communication Technologies*, 2(1).

Li, W. and Joshi, A. (n.d.). 'Security Issues in Mobile Ad Hoc Networks - A Survey.

Lidong, Z. and Haas, Z. (1999). Securing ad hoc networks. *IEEE Network*, 13(6), pp.24-30.

Ning, P. and Sun, K. (2006). How to misuse AODV: a case study of insider attacks against mobile ad-hoc routing protocols. *Ad Hoc Networks*, 3(6), pp.795-819.

Perkins, C., Belding-Royer, E. and Das, S. (2003). *Ad hoc on demand distance vector (AODV) routing*. [Internet Draft] draft-ietf-manet-aodv-13.txt.

Sanzgiri, K., Dahill, B., Levine, B., Shields, C. and Belding-Royer, E. (2002). A secure routing protocol for ad hoc networks. *10th IEEE International Conference on Network Protocols*.

Treesa, N. (2013). A Survey on Intrusion Detection Systems in Manets. *International Journal of Advanced Research in Computer and Communication Engineering*, 2(5).

Viranda, V. (n.d.). Intrusion Detection System (IDS) for Secure MANETs: A Study. *International Journal Of Computational Engineering Research (ijceronline.com)*, 2(6).

Yi, J. (2015). *draft-ietf-manet-nhdp-sec-threats-06 – Security Threats for the Neighborhood Discovery Protocol (NHDP)*. [online] Tools.ietf.org. Available at: https://tools.ietf.org/html/draft-ietf-manet-nhdp-sec-threats-06#page-18 [Accessed 4 Jun. 2015].