Volume 5, Issue 8, August 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Security Attacks and Solutions in Mobile Ad Hoc Network: Survey Paper

Samuel Eding*, Humayun Bakht, Philip Evans
London School of Commerce,
United Kingdom

Abstract— Mobile ad hoc networks are particular types of multi-hop wireless networks that do not have central management, are self-configurable and highly dynamic. Due to these unique properties of MANETs they are more vulnerable to many attacks than traditional networks. This paper investigates the criteria required for a perfect secure mobile ad-hoc network system. In this context, this work elaborates on security attack in MANET besides critically analyzed dominant security schemes in this area.

Keywords— Mobile ad hoc networks, secure routing protocols, MANETs, attacks in MANETs

I. INTRODUCTION

Mobile ad hoc networks (MANETs) are self-configurable and highly dynamic multi-hop wireless networks operating without the aid of a centralized infrastructure. In a mobile ad hoc network each node can move independently and spontaneously, therefore leading to constant changes in the network topology. Moreover, mobile ad hoc network can get built and destructed dynamically and unpredictably. Due to the lack of any central administration it is difficult to know an insider or outsider of the network. This makes a challenge to differentiate between illegal or legal participant of the network. In the light of the above enumerated properties, there is a need of designing an effective security solution for mobile ad hoc network systems.

Mobile ad hoc networks need particular flexible technologies in order to establish communications in situations that require a complete decentralized network lacking a fixed based station. Such environment can be seen in disaster areas, in battlefield areas and also in private events and meetings [1]. Due to the fact that it is difficult to spot a genuine participant from the malicious node in the network, it is therefore likely that the network can suffer security attacks at any time. These security attacks can be categorized as passive or active depending on whether the network's operations are disrupted on or not [2].

Some of the well-known routing protocol such as AODV, DSR, DSDV and many more have not been designed taking into account the security aspect of the network [5-10]. For example all those aforementioned protocols have to share the IDs of the nodes in order to have a full cooperation on the network for route building. This situation can lead to multiple attacks on nodes and disrupt the whole network [15]. Therefore, there is need to have a full secure routing protocol that can take into account all the security aspects of mobile ad hoc network

II. SECURITY CRITERIA IN MANETS

The perfect or ultimate security solution for MANETs should provide some key aspects of security such as integrity, authentication, confidentiality, non-repudiation, availability and anonymity to mobile nodes in the network. In order to achieve this objective, the designed security solution should try to secure the entire network stack. According to [8-9], it should be mentioned that fulfilling all the security criteria in only one solution is not an easy task and can sometimes reduce the performance of the network. Below is the description of some of the key security criteria.

Availability: This requirement is implemented to ensure that all the important services are provided by a node at any moment whenever they are required, whatever be the case. Furthermore, the availability requirement in a network means that all its resources and services must be accessible, even in a situation of network attack.

Confidentiality: This requirement is introduced to prevent unauthorized nodes (intermediate nodes) from accessing the inside of a message. Confidentiality does not only procure survivability to users' information for instance strategic or tactical military information but, also to the routing information. In order to make a network more confidential a well-known encryption technique mixed with an appropriate key management system should be used.

Integrity: This requirement is included in order to prevent unauthorized nodes to modify, delete, remove, record, corrupt or re-transmit data using malicious attack. Data integrity is a key requirement for security when a company uses sensible information. For example banking sector data, armed forces data or transport (e.g. trains or planes) data are really sensible. Therefore, a small modification on those data can lead to severe damages.

Authentication: This requirement is used to make sure that both the sender and receiver nodes are not impersonators but are genuine. If authentication is not properly implemented, it is difficult to implement the other ones. For example, let

assume that in order to implement confidentiality a symmetric-key has been used to encrypt a transmitted message among two nodes. If the authentication requirement is not properly implemented, one of the two nodes can be compromised. As a result of that all the encrypted material (encryption algorithm and the key) will be readable by that node.

Non-repudiation: when this requirement is implemented, it helps to ensure that both the receiver and the sender will not deny the fact they have receive or send data to or from other mobile nodes. If this requirement is properly implemented, detecting and isolating comprised mobile nodes becomes an easy task.

Non-impersonation: when requirement is well implemented, a node cannot pretend to be another authorized node to have access to important information in the network

III. ATTACKS IN MANETS

There are several kinds of attacks that can be carried out on mobile ad hoc networks. In general, those attacks can be categorized in two known as passive and active attacks [17].

A passive attack is an attempt performed by a misbehaving node in order to identify and acquire certain information transferred over the network without interrupting its operations. Detecting a passive attack is a complex task because the network processes are not disrupted.

Opposed to passive attacks that are not interrupting the networks operations, active attacks aim at altering, injecting, deleting or destroying packets being transferred over the network. Such attacks are able to be performed by either external or internal attackers. Below is the description of some of the well-known attacks.

Denial of service. Denials of services are active attacks that try to make resources not available to those who want to use them. In this attack the access to the majority of services offered on the mobile network are prevented by the attacker. According to [9] it exists different ways to carry out a denial of services, but all of them are causing similar damages. Generally, denials of services are carried out in standard manner which consist of overflowing the main servers with useless packets; therefore leading to a crash or an interruption of the operations of the system. According to [11-17] the fact that mobile ad hoc networks have certain particular characteristics which differ them from other networks, thus, it makes possible for an attacker to carry out denial of services in other ways than the traditional ones. This can be done at every layer of the protocol stack.

Impersonation. In this attack the attacker on a node with limited access to certain network resources, tries to imitate the behaviors of one of the node with full access to resources, in order to simply read the inaccessible information or to disturb the network performance by inserting wrong routing data [4]. An example of impersonation attack is man in the middle attack. When this is carried out an attacker is able to read of modify packets going from one genuine node to another one without making them notice that such a thing has happened.

Disclosure. A node which has been compromised can reveal secret information to another user which is outside the network. For that reason, the network should be able to fight against attacks such as eavesdrop which are the kinds of attacks trying to reveal private information that are being passed over the network.

Repudiation. Basically, repudiation attack occurs when a node does not want to accept that it has participated in a communication or specific action carried out on the network.

Routing attack. Generally speaking, it is on the network layer that routing attacks are performed. The aim of this attack is to make the network services not to be available. In the literature many examples of routing attacks are discussed. According to [11 - 13], the most common routing attacks are the following:

- ***Routing table overflow***. The key objective of this type of attack is creating and overflowing the routing tables. As a result of this new genuine routes cannot be created. All the packets which are transmitted are redirected through false routes or to inexistent mobile nodes.
- ***Location disclosure***. Normally, information such as node's location or structure of the network is not disclosed. But when Location disclosure attack is performed, it becomes able to read such information.
- ***Black hole attack***. It is an attack in which the compromised node which wants to intercept packets of a specific node advertised themselves to other nodes as having the best route to that destination. As a result all the nodes in the network wanting to send packets to that destination will be obliged to route them through that malicious node.
- ***Packet replication.*** The aim of this attack is to reproduce old packets. It happens when a specific node reproduce many packets that are already been sent. The result of this is a confusion created in the routing process and also a waste of network resources such as bandwidth or battery power.
- ***Sleep deprivation.*** Due to the fact that mobile ad hoc networks have that characteristic of power limitation, a malicious node can use that aspect with the aim of overusing that battery power. It will accomplish this by sending unnecessary packets to a particular node just to keep it receiving and routing packets.
- ***Blackmail***: This attack is carried out on network using routing protocols that tend to list bad and good nodes based on their participation in the network flow [1]. A single or many compromised nodes can deliberately list one or multiple nodes as bad. Therefore, their trust level will reduce and they will not be used in the traffic. Using the concept of trusting routing protocol or non-repudiation property in the network can be very useful in tackling this attack.
- ***Rushing attack***: This is another type of attack carried out on routing protocol. It is the fact of applying denial of service attack against ad hoc on demand routing protocols. When this attack is successful on these routing protocols, they become unable to discover a route with more than two hops.

Wormhole attack: This attack is one of the complicated one in mobile ad hoc network due to the fact that it is carried out by two or more cooperative malicious nodes that participate in the network [9]. In this attack, one node captures some routing traffic from one part of the network and tunnels them to a different node in another part of the network that shares private information with the first one. When it reaches the targeted nodes, this one reinserts that information into the routing traffic. Consequently, all the routes created through that traffic will be under the control of the malicious nodes. One solution to tackle this attack is the use of packet leashes techniques.

Masquerading attack: In this attack, a node can masquerade another node and therefore join the network. This attack is somehow difficult to achieve since the attacker needs to know the topology of the network as well as the ID of the nodes that it wants to impersonate.

Passive listening and traffic analysis attack: With this attack, the aim is not to disrupt the network, but only to carry a passive gathering and analysis of routing information passing over the network [12].

In the light of the above discussion it can be concluded that attacks in MANETs poses a serious threats. That is why, security should be taken into account at every stage in the design of such networks. The following table, table 1 summarises the different attack classified by layer of communication.

Table1: security attacks grouped by network layers

Table1: security attacks grouped by network layers

Layer	Attacks
Application Layer	Repudiation attack and data corruption attack
Transport layer	Session hijacking, SYN flooding, Traffic analysis, monitoring, disruption MAC (802.11), WEP, Weakness Jamming, interceptions, eavesdropping
Network layer	Routing attacks, resource consumption, black hole, Byzantine, flooding, location disclosure attacks, wormhole
Data link layer	monitoring, WEP weakness, disruption MAC (802.11), Traffic analysis
Physical layer	Interceptions, eavesdropping, jamming

IV. SECURITY SCHEMES FOR MANETS

It is difficult to differentiate between malicious network activities and specific problems associated with an ad hoc networking environment. In a mobile ad hoc network, malicious nodes may enter and leave the immediate radio transmission range at random intervals or may collude with other malicious nodes to disrupt network activity and avoid detection. Certain malicious nodes may behave maliciously only occasionally, further complicating their detection [3]. Dynamic topologies of mobile ad hoc networks make it tough to get an overall view of the network and any estimation can come to be quickly outdated. Though multiple secure solutions have been designed to address the problem of security in mobile ad hoc networks, none of them none of them has successfully fulfil all the security criteria.

A. Link layer security schemes

Link-layer security schemes protect the one-hop connectivity between two direct neighbours that are within communication range of each other through secure MAC (medium access control) protocol. The majority of security solutions designed for mobile wireless devices is offered by data link layer security schemes implemented in IEEE 802.11 and Bluetooth standards. Some schemes based on IEEE 802.11x supporting diverse authentication modes have also been proposed by the Target Group (TGi). Bluetooth specification includes a set of security profiles for service-level and for data link layer security [8-9].

B. Authentication schemes

This type of security scheme focuses on all type of authentications going from simple authentication schemes that includes resurrecting duckling [5], zero configuration (environment where there is not central infrastructure), face to face authentication (authentication using key or cryptographic approaches). Distributed scalability in authentication is achieved in mobile ad hoc networks when the notion of local trust model is combined with the authentication technique.

C. Cooperative schemes

This type of schemes tries to address the problem of node selfishness in all aspects. This is achieve by the creating and introducing into all the network transactions a specific type of virtual currency that helps to monitor nodes participation in the network. An example of such scheme that uses virtual currency or token has been implemented by [8-9].

D. Secure Packets schemes

Consisting on detection and reaction mechanisms, secure packets schemes help to address the issues generated by malicious nodes that fail to correctly forward packets to a given destination. Examples of such security schemes can be watchdog and path rather which has been implemented by [8-9].

E. Intrusion Detection Techniques

The principle behind intrusion detection system schemes (IDS) consists of capturing and analyzing data traffic in order to provide clear evidence that the network is under attack [18]. Depending on the type audit data that has been used, intrusion detection schemes can be classified as network or host based. An intrusion detection scheme is said to be network based when the captured packets are taken from the gateway of the network. These are packets that are going through the network through the network interface card. Whereas an intrusion detection scheme is said to be host based when the data that are analyzed are events generated by the software or users on the nodes. To discover that something is wrong in the network, intrusion detection schemes can used techniques such as misuse detection or anomaly detection. But both techniques depend on actions such as packets sniffing and later analyzing them [4]. In [18], Zhang and Lee designed a model for intrusion detection system in which each node in the MANET detects and give response using agents called IDS agents.

In mobile ad hoc networks, the fact of not having a fixed or centralized infrastructure where real traffic monitoring is performed makes data capturing limited to the radio-range of nodes. As a result of this, only local network issues can be detected. This does not give a real time overview of what is happening in the network. That is why applying sole intrusion detection system in mobile ad hoc networks is not really efficient. For a better result, this should be used to complement other techniques such as prevention schemes like secure routing, authentication or cryptographic techniques and have distributed and cooperative properties. Another way of improving the efficiency of intrusion detection schemes is incorporate it into the different layers of the network using a cross-layer approach.

F. Secure Routing Schemes

Routing functionalities in mobile ad hoc networks are not performed by routers as it is in normal wired networks. These functionalities are distributed over the network to all the nodes which are acting terminal and as routers for other devices in the network. Providing security in such environment is not an easy task due to the fact that the network can be subject to many attacks. The design process of most of the routing protocols does not take into consideration the aspect of security. Implementing security techniques in order to tackle attacks that might occur on the network particularly attacks perpetrated at the network layer must be done fulfilling a number of specific requirements [9].

An example of attack that can be carried out at the network level in mobile ad hoc network is wormhole attack. As seen above, this attack aims at completely disrupting the routing operations. Many approaches designed to tackle this attack have used the concept of packet leashes which is a secure packet forwarding technique [9]. But many researchers have also developed secure routing protocols to handle this issue. These protocols use techniques such hash functions, digital signature and other types of encryption.

Table 2 below illustrates some of the main routing properties as well as the tools used to achieve those properties.

Table 2: Security properties and techniques used to fulfil them

MANETs security properties and techniques	
Authentication	Password, digital certificate
Authorization	Credentials
Integrity	Digest, digital signature
Confidentiality	Encryption
Non-repudiation	Digital signature
Timeliness	Timestamp
Ordering	Sequence number

The next subsections describe some of the well-known secure routing protocols.

SRP. The secure routing protocol (SRP) is a routing protocol that helps to protect against all type of attacks that aim at disrupting the process of route discovery in the network. By doing this, it helps to maintain the correct topology of the network [15]. The mechanisms employed in this protocol helps to make sure that fabricated routes or the replayed ones should not reach the querying node [20]. One of the drawbacks of this routing protocol is that it increases the overhead of the packets and adds more computation due to the fact that the added overhead contains an encryption technique. Moreover this protocol cannot perform well against security attacks such as selfish and wormhole attacks.

SAR. The security aware ad hoc routing protocol (SAR) is a routing protocol that uses different level of trust amongst nodes in order to route data from one source to a specific destination [9]. According to the trust hierarchy being used, different levels of trust can be define among nodes. At every level there is a common key which is share among nodes. This key is used to encrypt and decrypt information. The same key can also be used to communique with nodes at higher levels of trust. One drawback of such a protocol is that it make use of so many keys. This is because every level has different keys.

SEAD. Designed with the aim of addressing attacks such as denial of services and resource consumption, the secure efficient ad hoc distance vector (SEAD) routing protocol is an extension of the destination sequence vector routing protocol DSDV [21]. Motivated by DSDV-SQ routing protocol, SEAD has been designed to tackle issues related to the modification of sequence number and metric field in the routing packets. Security is implemented in this protocol by using one-way hash chain. This allow another node to authenticate the sequence number and metric field of routing table

update massages. Moreover the destination also authenticate the source node in order to make sure that it is not a malicious one. One of the drawback of this protocol is that it does not implement a mechanism that can stop an attacker of modifying some field such as next hop or destination in the routing message update. Furthermore, SEAD has not implemented a mechanism that can deny an attacker from using the same sequence number or metric taken from another node.

ARAN. The authenticated routing for ad hoc networks (ARAN) is routing protocol that uses cryptographic certificates in order to protect the network against attacks carried out by malicious nodes in the network. This secure routing protocol tries fulfil security criteria such authentication, integrity and non-repudiation [9]. The steps involved in the process of securing are firstly certification followed a mandatory end-to-end authentication. Optionally there is last stage that consist of providing secure shortest path

ARIADNE On-demand secure routing protocol (ARIADNE) is a secure routing protocol that is implemented from another protocol called dynamic source routing protocol (DSR). To achieve security, ADRIANE uses symmetric encryption [3]. This routing protocol provides point-to-point authentication of all routing messages by means of a share key and a MAC (message authentication code). Before establishing a communication, each sender needs to have a shared key between itself and the destination. One of the drawback of this routing protocol is that it is unable to protect against certain attacks such as wormhole.

SAODV. Based on the AODV protocol, SAODV is a secure routing protocol that is effective in combatting attacks such as black-hole when this is only caused by a single node [6]. The SAODV protocol make use of techniques such authentication and hashing in order to make sure that malicious nodes are not sending or receiving packets in the network. This is done by implementing an asymmetric encryption and hash function to the routing messages. This protocol limits as well the number of route reply that can be generated by a single node. One of the drawbacks of this routing protocol is that it uses lot overhead, and is unable to protect against attacks perpetrated by a group of collaborating nodes.

TAODV. Also based on AODV, trusted AODV protocol is a secure protocol that was implemented by [8]. Security is achieved in the network by the usage of trust amongst nodes. Based on the trust level of a particular node, TAODV will define the encryption level that needs to be used by means of a specific application [9]. According to [14], the main idea behind this protocol is to use trustworthiness in order to send or hide packets in the network. The more a node is trusted, the less its packets are going to be hidden in the network. One drawback of this protocol is that, it is unable to protect against attacks such as wormhole attack and impersonation attack.

SecAODV. Patwardhan and Iorga designed a secure routing protocol based on AODV called SecAODV [7]. This protocol makes use of static IPv6 addresses. A secure communication is therefore established by using some statistical techniques and encryption identifiers to bind the IP address to the provided key. This protocol also provides an intrusion detection system (IDS) mechanism. One of the drawbacks of this technique is that, the protocol is too sensitive on the hello time and all the variables around it.

V. CONCLUSION

Due to their infrastructure-less architecture and the dynamic nature of their topologies, mobile ad hoc networks are difficult to get designed and implemented securely. In order to fulfil all the security goals in their deployment, MANETs need to be designed efficiently. The growing number of applications of mobile ad hoc networks lay emphasis on the need for tough privacy and security mechanisms. This paper highlights well-known security issues and security solutions encountered in mobile ad hoc networks. It describes security goals, potential threats or attacks and describes key security mechanisms and schemes.

Though many solutions to tackle security issues in MANETs have been implemented, we are still far from having solve all the problems. Researchers in the domain of cryptographic authentication and key distribution are still working to provide algorithmic solutions that are going to be efficient as well as using less message overhead. Many solutions have been implemented in order to solve a particular problem. Therefore, they are not able to tackle other issues. Designing proper mechanisms to self-enforce and enhance privacy policies in mobile ad hoc networks is also being studied by many researchers around the world.

REFERENCES

[1] A. Al-Bayatti, H. Zedan, and A. Cau, “Security solution for mobile ad hoc network of networks (MANON)”, ICNS ’09. Fifth International Conference on in Networking and Services, pp. 255 –262, April 2009.

[2] A. Hamza, T. Alwada’n, H. Janicke and A. Al-Bayatti, “Data Confidentiality in Mobile ad hoc network”, International Journal of Wireless & Mobile Networks (IJWMN) Vol. 4, No. 1, Feb 2012

[3] Y.-C. Hu, D.B. Johnson and A. Perrig, SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks, in: WMCSA’02

[4] A.H. Shabaan, H. El Zouka and M. Abou El Nasr, “Intrusion Detection System in wireless Ad-hoc Networks Based on Mobile Agent Technology", IEEE 2011 2nd International Conference Computer Engineering and Technology, Chengdu, Vol.1, p.470-474,16-18 Ap.2010

[5] Charles E. Perkins, Elizabeth M. Belding Royer, Samir R. Das, “Ad hoc On-Demand Distance Vector (AODV) Routing” RFC 3561, November 2003.

[6] M. Guerrero Zapata, “Secure Ad hoc On-Demand Distance Vector (SAODV) Routing” The internet engineering Task force September 2006.

[7] Patwardhan A, Parker J, Joshi A, Iorga M and Karygiannis T. "Secure routing and intrusion detection in ad hoc networks". In : *Proceedings of the 3rd IEEE International Conference on Pervasive Computing and Communications (PerCom 2005)191 – 199*.

[8] Nekkanti RK and Lee CW, **"**Trust based adaptive on demand ad hoc routing protocol" *Proceedings of the 42nd annual southeast regional conference* 88–93.

[9] N. HimadriSaha, B. Debika, B. Bipasha, M. Sulagna, R.t Singh and D. Ghosh, " A review of attacks and secure routing protocol in MANETs", International Journal of Innovative Research and Review, Oct2013, *pp12-36*

[10] Sanzgiri, K., Dahill, B., Levine, B. N., Shields, C., & Belding-Royer, E. (2002). A secure routing protocol for ad hoc networks. *Proceedings of the 10th International Conference on Network Protocols (ICNP'02).*

[11] Yi S, Naldurg P and Kravets R (2002). Integrating quality of protection into ad hoc routing protocols. In: *Proceedings of the 6th World Multi-Conference on Systemic, Cybernetics and Informatics (SCI 2002)*

[12] Yan Z, Zhang P and Virtanen T (2003). Trust evaluation based security solution in ad hoc networks. *In Proceedings of the 7th Nordic Workshop on Secure IT Systems* (NordSec 2003).

[13] Perkins C and Royer E (1999). **"**Ad hoc on-demand distance vector routing". In: *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 1999)* 80–100.

[14] Papadimitratos, P., & Haas, Z. (2003). Secure link state routing for mobile ad hoc networks. *Proceedings of IEEE Workshop on Security and Assurance in Ad Hoc Networks*.

[15] Papadimitratos, P., & Haas, Z. (2002). "Secure routing for mobile ad hoc networks". In *Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002)*, San Antonio, TX, January 27-31, 2002

[16] Hu, Y.-C., Johnson, D. B., & Perrig, A. (2002b). SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. *Proceedings of Fourth IEEE Workshop on Mobile Computing Systems and Applications (WM-CSA'02*).

[17] Zhang Z (2011). Mobile Ad-Hoc Networks: Protocol Design. Chapter 22: A Novel Secure Routing Protocol for MANETs, University of Southern Queensland, Australia 455-466. Available: www.intechopen.com, Publisher InTech, Published online 30, January, 2011, Published in print edition.

[18] S. Basagni, M. Conti, S. Giordano, and I. Stojmenovic, "Mobile ad hoc networking," Wiley-IEEE Press, Aug. 2004.

[19] Zhang, Y; Lee, W and Huang Y.-A. (2003). "Intrusion detection techniques for mobile wireless networks", Wireless journal (ACM WINET), Vol. 9, No. 5, September 2003, pp. 545-556, ISSN: 1022-0038.

[20] Sanzgiri, K.; Dahill, B.; Levine, B. N.; Shields, C. & Belding-Royer, E. M. (2002). A secure routing protocol for ad hoc networks. Proceedings of IEEE International Conference on Network Protocols (ICNP'02), pp. 78 – 87.

[21] Johnson, David B., and Adrian Perrig, with Yih-Chun Hu. "SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks." *Ad Hoc Networks* 1.1 (2003): 175-192.

