Analysis of MANET Security –Challenges, Threats & Solutions

C. P. Agrawal
Computer Deptt, MCRPSV, 38 B,
Press Complex, Bhopal (MP), INDIA
919425602012
agrawalcp@yahoo.com

O. P.Vyas
IIIT Allahabad, Deoghat-Jhalwa,
Allahabad(UP) 211012, INDIA
915322922218
dropvyas@gmail.com

P. Udaykumar
Dept.of M.C.A, RCET (Rungta)
Bhilai (CG), INDIA
919893263785
uday_uday06@yahoo.co.in

ABSTRACT

The Mobile Adhoc Networks (MANETs) have applications in the practical situations where the possibility of providing infrastructure networking is difficult. With this development they have been submitted to several security threats which require a serious attention, remedies and dependable deployment of secure protocols. In general, the protocols assure that the neighboring nodes in the network are reliable and trustworthy. In practical situations, this assumption might not hold good due to presence of intruders who might mal-function or paralyze MANETs by manipulating the messages flowing in the network creating various security hazards. The issue require keen analysis due to the fact that the MANET do not satisfy security concepts in wired networks, especially, due to leakages because of the routing protocols in MANET. This paper analyses various security issues like challenges, requirements etc. Further it gives their classification, OSI layered analysis and finally surveys various secure protocols available with their technologies.

Categories and Subject Descriptors

C.2.1 Network Architecture and Design - *Wireless communication*
C.2.2 Network Protocols -*Routing protocols*

General Terms

Security.

Keywords

MANET, OSI Layer, Protocols, AODV, DSR

1 FUNDAMENTAL SECURITY REQUIREMENTS

In order to get an assured secure communication in MANET the network must ensure basic requirements [2, 6]. The routing messages are not altered in communication chain. There is no formation of communication loop in the transit. The route regulating is not spoofed. Fake and fabricated routing messages are not injected into the network. The routs are not redirected to an attacker node The intruder and unauthorized nodes if any are immediately identified and excluded from the safe nodes as well as the route computation tables. The nodes, which are authorized in the network, but have been modified by intruders or viruses to malfunction are rather identified and secluded. The stability against attack by resuming normal safe operation is achieved within a short time span. Confidentiality of the nodes and the networks topology is maintained .

2 CHALLENGES TO MANET SECURITY

The security issues in MANET becomes more complicated, because of the several compelling situations, as indicated below[2, 3].

Scarcity of resources - The mobile nodes are often at limited resources availability including the battery power, computational power, memory, speed etc. Due to this restrictions the security solutions consuming higher resources e.g. public key cryptography, are not deployable practically.

Physical security threats- The mobile wireless networks are more open to physical security threats. Due to small size of nodes and permitted mobility, they are more prone to stealing and physical mishandling .

Topological variations - Due to the transient and moving nature of nodes the locational dependency is less assured.

Lack of regulating authorities - Unlike the infrastructure-based network in MANET the central regulating authorities do not exist in MANET.

Shared wireless medium - In MANET the wireless based of communication is broadcast based, hence all data is available to all the nodes for tempering, resulting more complexity & challenges to security..

Insufficient rules for association - The MANET lacks proper authentication rules and mechanisms for associating nodes in the network. Unlike in general network, an intruder can easily join the network and create security hazards.

Hostile and insufficient operational environment - Since the MANET found more complications in environment like war fields , there are more hazards to security issues.

3 MAJOR ATTRIBUTES FOR SECURE PROTOCOLS

To achieve the laid down objectives of security, protocols are expected to fulfill the following attributes [3, 4, 6]

Confidentiality- To ensure that the information is accessible only to the intended destinations the routing and packet, the information must also remain confidential to safeguard from intruders.

Availability- It relates ensuring the availability of resources to the genuine nodes in the network. A possible security hazards is consuming the resources to disable or jam the network due to shortage of the resources.

Authenticity - It ensures that the supply or access of the resources is done only to the authorized parties. Without this authentication, an intruder can gain unauthorized access to resources or information.

Scalability- The security mechanisms must be able to handle the designated size of the network. This is essential as an natural outcome of the fact that the networks have tendency to expand over time.

Ownership - Neither the sender nor receiver should deny the ownership of message sent or received.

Generosity – Nodes must be available to invest their resources for relaying the packets for assisting the other nodes in the network, rather than being miser in saving expensive resources for own usage.

4 CLASSIFICATION OF SECURITY ATTACKS ON MANETS

The resources scarcity, complexity and uniqueness of MANET result into higher vulnerability to security threats than the fixed infrastructure networks. To enable the objective of a secure system it is essential to understand different types of attacks, detect them and correctively overtake them [2, 7, 12]. They are classified in two main types. Active & Passive Attacks. In Active attacks, the normal operation of the network is active. The attacker has to actively participate in the on going network for disrupting the network performance, hence bears energy & cost to perform the attack.. It can destroy or alter the data communicated in the network. Effectively it degrades the performance or confuses the routing mechanism. The malicious nodes responsible for active attacks might be due to internal or external attacks. The internal attacks are through legitimate nodes of the network, but are malfunctioning or compromising against security. They are more difficult to be identified. On the other hand an external attacker is an unauthorized node intruding in the network. They are comparatively easy to be defended by means of firewalls, source authentication or encryption mechanism. On the other hand the Passive Attacks do not disrupt the network functioning. Mainly the requirement of confidentiality get violated and the attacker spoofs the messages. It is more difficult to detect such attacks due to the continuation of the normal network functioning. The best mechanism of defense is powerful encryption algorithm Based on the damages prone from attacks, they are grouped in following categories.

4.1 Modification Attack

In this attack the intruder, in addition to gaining access to the resources, can temper with them illegally. It can lead to redirecting traffic towards a different destination, dropping out the traffic or routes through longer routes/ loops. The attack can cause false identification of healthy node or malicious node, blackmailing the healthy nodes. Few examples in this category are listed.

Misrouting attack- A non-legitimate node which direct a routing message or data to incorrect destinations.

Detour Attack- It adds a number of virtual nodes in route, diverting the traffic through a longer/ malicious node. The attacking node itself can save energy by forwarding packets.

Denial-of-service attack – It can affect denial-of-service to legitimate and authorized users.

Blackmail attack - It causes false identification of a good node as malicious node. An attacker may blackmail a good node and tell other nodes in the network to add that node to their blacklists as well, thus avoiding the victim node in future routes.

Byzantine attack- This type creates routing loops or longer paths or packet dropping misroute attack. Here a compromised intermediate node or a set of compromised intermediate nodes collectively carry out attacks such as creating routing loops, routing packets on non-optimal paths and selectively dropping packets. Since in such attacks the network would seem to operate normally Byzantine failure are hard to detect.

4.2 Fabrication Attack

In this type, an unauthorized node gains access, generates false routing messages or inserts counter fate objects like routing updates or error messages to disturb the network operation or consume its resources. Few examples are discussed in this section.

Routing table or cache poisoning- In this type a malicious node sends incorrect routing updates resulting in to sub optimal or in accessible network functions.

Routing consumption attack - In this type a malicious node attempts in consuming the network resources o disrupt its functioning.

Rushing attack- An attacker node which receives any route request packet from the source node floods the packet quickly through out the network before other nodes which also receive the same route request packet can react. Nodes that receive the legitimate route request packet assume those packets to be the duplicates of the packet already received through the attacker node and hence discard those packets. Any route discovered by the source node would contain the attacker node as one of the intermediate nodes. Hence the source node would not be able to find secure routes

Routing table overflow - In this type, the attacker broadcasts routes to fictitious or unauthorized nodes present in the network resulting into overflow of routing table, finally disabling new routes to the authorized nodes.

Grayhole attack - In this type, the attacker drops the data packets, but allows control of messages to be routed in the network. The process makes it very challenging to detect the attacker.

Blackhole attack- In this type a malicious node enters the path finding process by falsely advertising as shortest path to the destination mode. This result into failure of data packets delivery to the destination node. The attacker can also monitor and analyze the data flow, to find activity patterns for further enhance the insecurity.

4.3 Reply Attacks

In this style the attacker re-transit data to produce an unauthorized result. Few examples are listed below.

Warmhole Attack - In this type two compromising nodes can communicate creating vertex cut of nodes by recording a packet at one location. They can drop packets and selectively forward packets to avoid detection .

Tunneling Attack - In this type two or more nodes communicate encapsulated messages along the existing data route. This results in convincing the receiver that the path involving attacker is the shortest one. This result in prevention of honest intermediate nodes in participating the routing. The routing metrics misrepresent the path length. It can be detected by time delay metrics .

4.4 Impersonation Attacks

The absence of authentication mechanism for data packets can lead to impersonation of a malicious node by misrepresenting its identity in the network . Say by IP altering the network topology is prone to spoofing.

5 ILLUSTRATION OF SECURITY OF POPULAR ROUTING PROTOCOLS

5.1 AODV Protocol

AODV (Ad hoc On Demand Distance Vector) Routing Algorithm is a Reactive algorithm which routs only towards nodes which needs to communicate. The routing messages do not contain information about the entire route path, but only about the source and destination resulting into constant size. Its uses destination sequence number to ensure absence of loops. The protocol has less memory requirements and less traffic load along the links. An intruder may advertise a route with small distance metric than the original distance or advertise a routing update with large sequence number, effectively invalidating all routing update from other nodes. It has no security mechanism against such situations. Further, a malicious node can impersonate by forging RREQ (or RREP) that its address as originator (or destination) address to paralyze the entire network. It is also possible that a node denies to forward certain request or does not require the request or does not forward data messages creating more difficult security hazards difficult to be detected. It can also cause black hole attacks due to forgiving RREP misleading a node to be false destination. It is also subjected to redirected with modified Hopcount attack. This happens, because the protocol use a Hopcount to determine a shortest route. The malicious node can resent Hopcount to zero or infinity causing route deviation from the destination. A possible enhancement is secure AODV which has, certified public keys along with cryptography for safety. However, this results into a higher load on the protocol.

5.2 DSR Protocol.

The DSR (Dynamic Source Routing) protocol is an on-demand protocol. The source sending a packet includes complete sequence of nodes in the packet header through which the packet is to be forwarded. These routes lack integrity check, leading to denial-of-services attack due to the altering the sources route in packet header. The route maintenance mechanism involves forwarding node to ensure confirmation of the packet received by the next hop, along with path in case the confirmation of receipt after defined maximum attempts is not received, which creates an error message. This leads the possibility of loops creation due to insufficient safeguards.

6 SECURITY ANALYSIS WITH RESPECT TO OSI LAYERS

The issues of security related to the five layers of mobile ad-hoc networks and the related countermeasures are summarized in this section.

6.1 Physical Layer

For MANETs at this layer intruders can gain access to the wireless media, intercept data or disrupt the network physically. It is very crucial location, for security as it is prone to many types of attacks at this level. The best practice to safeguard against this layer attacks is the use of a two spread spectra technology, which changes frequency in a random manner or utilizes a wider spectrum making it more difficult to capture signal. For creating difficulties for the malicious user while trying to intercept the radio signals, for cases where the hopping pattern or spreading code is unknown to the eavesdropper two methods are employed. The signals are made unintelligible duration impulse noise to the eavesdroppers by Frequency Hopping Spread Spectrum (FHSS) and each data bit in the original signal converted by multiple bits in the transmitted signal through 11-bit Barker code Direct Sequence Spread Spectrum (DSSS). To capture and release the content of transmitted signal, the attacker must know frequency band, spreading code and modulation techniques. The main attacks at this layer are listed below.

Eavesdropping is the attack, in which an unauthorized intruder reaches messages in the network. It also creates possibility of injection of fake messages in the network, called impersonating. This is very common, due to the ease of unauthorized tuning to the operational frequency due to use of wireless media or RF Spectrum.

Jamming is another common attack, in which the radio signals are lost or corrupted by use of a powerful transmitter, which is strong enough to overpower the network. Pulse and random noise are also used for signal jamming

Interference is the attack in which the radio signals are corrupted by insertion of powerful noise signals .

6.2 Data Link Layer

The security threats in this layer are mainly due to possibility of disrupting the cooperation of the protocols of this layer. The protocols must be maintained with the high powers with an open multi point peer to peer network architecture. E.g the IEEE 802.11 Medium Access Control (MAC) protocol employs distribution based on either of the two coordinate functions, the fully distributed access or the central access protocol called Distributed Coordination Function (DCF) and Point Coordination Function (PCF) respectively . A selfish or malicious node can also interrupt and disrupt the back off mechanism. It is also vulnerable to denial-of-service attacks due to corruption of frames by adding extra bits or ignoring the on going transmission The Wired Equated Privacy (WEP) security scheme at this level, is vulnerable to message privacy and integrity attacks due to lack of key management feature. Similarly, the possible of non-cryptographic integrity may lead to message privacy and integrity attacks.

For providing security against these possibilities the back off scheme can be modified with back off timer provided from the receiver instead of an arbitrary timer value used earlier. The counter measures against WEP limitations are implementing RSN / AESCCMP. the threats of resource consumption can be addressed by ERA-802.11 scheme, to most extend. Similarly the weakness of WEP is handled by in 802.11i/WPA & RSN/AESCCMP.

6.3 Network layer

This layer plays a very crucial role in ensuring the over all network security. It is this layer responsible to establish an optional route between the communicating nodes through the routing protocols. The best line of defense is employment of secure routing protocol. The wormhole attacks can be detected by an unalterable and independent time delay or geographical location physical metric (eg. packet leashes, IPSec to provide certain level of confidentiality. To overcome blackhole attack, the ability to reply in a message of an intermediate node is disabled, so all reply messages should be sent out only by the destination node. The source authentication and message integrity mechanisms (eg digital signature, message authentication code (MAC), hashed MAC (HMAC), one-way HMAC key chain) are employed to prevent the active attack like modification of routing messages. The secure routing protocol like ARAN may also be used to protect from various attacks like modification of sequence number, modification of hop counts, modification of source routes, spoofing, fabrication of source route. The major attacks at this layer are indicated below.

Routing messages flooding attack like Hello, RREQ or ACK floodings .

Routing Cache Poisoning Attack involving broadcast of spoofed packets with source route to a node via itself. This misupdates the routing tables by deletion or false injection of information.

Routing Table Overflow Attack involves an excessive route advertisement sent, overflowing the routing table. It is applicable in table driven protocols only.

6.4 Transport layer

This layer of the protocols are responsible for reliable packet delivery, congestion control, flow control and providing end-to-end connections. The major issue of concern are authentication. The layer is also susceptible to SYN flooding or session hijack attacks similar to Internet TCP model. The flooding can be created due to long number of semi open PCP connections over the target node. A malicious node can send MSN to the target node which sends back acknowledge signal and awaits for its response. The flooding due to this hand shake overflows the buffer, disabling the system availability. The internet TCP protocol which does not readily suit to the MANET environment, can be modified to provide dependable security at this level, eg public cryptography. Few examples include - TCP explicit failure notification (TCP-ELFN), ad-hoc transmission control protocol (ATCP), TCP feedback (TCP-F) and ad hoc transport protocol (ATP) . The protocols can also make use of point to point communication through data encryption for enhancing the message confidentiality.

6.5 Application layer

At this layer applications needs to handle frequent connections, disconnection and reconnections with other peer applications and for different layers. The Application layer contains, user data supporting protocols like SMPP, TELNET, STTP, FTP having many vulnerabilities for intruders. The main attack of this layer are repudiation attacks causing denial of participation in communication or malicious code attacks like warm, virus, trojen horses, spyware etc. causing computer system or networking to damage or degrade the performance. Provisions of user authentication, packet filtering, network filtering, access control, accounting services by use of firewall provides protection against the some of the attacks. The application layer also detects a DoS attack more quickly than the other layers. Anti spyware software and use of Intrusion Detection System (IDS) can enhance the security against intruders pretending to be legitimate users.

7 SECURE PROTOCOLS FOR MANETS

Various researchers have proposed number of Secure Protocols for MANETS. Popular ones are indicated below [3].

Security Aware ad hoc Routing (SAR) secures the ad hoc routing protocols similar to traditional wired routing matrices where same security levels of nodes incorporate each other. The design approach is based on Quality of Protection (QoP) metric mechanism. Instead of discovering the shortest path between two nodes it can discover a path with desired security attributes, such as a path through nodes a particular shared key. It uses sequence numbers and times tamps to stop replay attacks in routing update packets Route discovered may not be the shortest route in terms of hop-count, but it is always secured. For this purpose to determine a secure route, the information in the routing messages must be protected against alteration that can change routing behavior. A node initiating route discovery determines the required minimal trust level for nodes participating in the query and reply propagation. Since only nodes at each trust level share symmetric encryption keys, intermediate nodes of different levels cannot decrypt in-transit routing packets or determine whether the required security attributes can be satisfied and drop them. Only the nodes with the correct key can read the header and forward the packet. So if a packet has reached the destination, it must have been propagated by nodes at the same level. Hence routes discovered assures quality of protection guarantees. One of the merits SAR has is that it can be implemented based on any on-demand ad hoc routing protocol with suitable modification. The security metric can be embedded into RREQ packet. It also showed the practical implementation and experimental data by mixing with AODV. Although SAR scheme provides protection of the routing protocol traffic, it does not eliminate false routing information provided by malicious nodes. Moreover, the assumed supervising organization and the fixed assignment of trust levels does not pertain to the ad hoc paradigm. SAR has also a lot of encryption overhead, since each intermediate node has to performs it, but provides excellent defends against modification and fabrication attacks.

Secure Efficient Ad hoc Distance Vector (SEAD) is a proactive routing protocol, based on the mechanism of One- way hash chains rather than implementing expensive asymmetric cryptography operations [11]. It prevents an attacker from forging better metrics or sequence numbers in routing update packets. As the fields such as destination, metric, next hop and sequence number are common with DSDV, it can be easily used with DSDV algorithm. The routing tables also maintain a hash value for each entry, both periodic and triggered. It does not prevent an attacker from tampering other fields or from using the learned metric and sequence number for sending new routing updates

Authenticated Routing for Ad-hoc Networks (ARAN) is an on-demand routing protocol based on Secure certificate server technology with heavy asymmetric cryptographic computations. It can detect and protect against malicious actions carried out by third parties and peers in particular ad-hoc environment. This protocol provides network services like authentication, message integrity and non-repudiation as a part of a minimal security policy. It is immune to rushing attack but prone to wormhole attack if accurate time synchronization is not available. It can be conveniently be used with AODV & DSR protocols.

Ariadne is an efficient on-demand ad hoc network routing protocol, based on One-way hash chains technology. It utilizes highly efficient symmetric cryptography. It provides point-to-point authentication of a routing message using a message authentication code (MAC) and a shared key between the two communicating parties. It prevents attackers from tempering uncompromised routes consisting of uncompromised nodes It is free from a flood of RREQ packets and cache poisoning attack, but it is immune to the wormhole attack and rushing attack. It can very well be integrated with DSR and TESLA protocols .

Sybil Attacks and Defenses Protocol (SADP) is based on Radio Resource Testing, Random Key Predistribution, One-way Pseudo Random Hash Function technologies. It is the first mechanism presently for protecting the Sybil attack.

8 WORMHOLE ATTACKS AND DEFENSES PROTOCOL (WADP)

is based on Packet Leashes, Merkle Hash Tree & One way Hash Chains technologies. When implemented with packet leaches, effectively stops wormhole and DoS attacks. It is not feasible in resource constraint networks due to the expensive cryptographic mechanisms implemente4d.

Cooperation Of Nodes - Fairness in Distributed Adhoc Networks (CONFIDANT) is a protocol which employs techniques of Reputation System, Path Manager, Monitor and Trust Manager. It has capacity to defend against attacks on packet forwarding and routing efficiently. It is vulnerable to spooling and Sybil attacks. It can be used with DSR efficiently.

Secure Routing Protocol (SRP) is based on Secure Certificate Server Technology. It provides prevention against attacks that disrupt the route discovery process and guarantees to identify the correct topological information. It lack of validation mechanism for route maintenance messages and is also prone to wormhole and invisible node attacks It is convenient to be implemented with DSR & ZRP protocols[8].

Timed Efficient Stream Loss-tolerant Authentication (TESLA) is based on One-way Hash Chain technology. It employs loose time synchronization and delayed time synchronization to provide secure broadcast. However it is vulnerable to DoS attacks as malicious nodes can create buffer overflow state. Also it lacks accurate time synchronization [9].

9 RUSHING ATTACKS AND DEFENSES PROTOCOL (RADP)

is based on Randomized Route Request Forwarding , Secure Neighbor Detection & Secure Route Delegation mechanisms. It prevents rushing attack to a certain level by limiting the total number of requests sent by a node and random forwarding. The network is still prone to rushing attacks if an attacker can compromise *k* nodes. It exerts higher overhead than other protocols. This is the only protocol that can defend against rushing attacks. It is used with DSR & ARIADNE protocols.

10 CONCLUSION

Though the Mobile Adhoc Networks (MANETs) have been the hot topic for the researchers since several years, but their practical implementations have failed to expand in the quantum that was envisaged. There have been compelling issues mainly related to security of the network. In this paper a detailed survey on the important aspects of MANET security has been performed. It covers various challenges to MANET security, technical requirements and attributes of security. Further the paper covers detailed classification of security attacks and explores various secure protocols along with their technical basis, advantages and applications. The security issues related to different OSI layers of the MANETs has also been analyzed along with the counter measures to be taken.

11 REFERENCES

[1] B. Wu, J. Chen, J. Wu, M. Cardei, “A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks,” Department of Computer Science and Engineering, Florida Atlantic University L. Zhou, Z.J. Haas, Cornell Univ., “Securing ad hoc networks,” IEEE Net

[2] H. Yang, H. Luo, F. Ye, S. Lu, L. Zhang, “Security in mobile ad hoc networks: challenges and solutions,” In proc. IEE Wireless Communication, UCLA, Los Angeles, CA, USA; volume- 11, Page(s): 38- 47, ISSN: 1536-1284

[3] J. Kong et al., “Providing robust and ubiquitous security support for mobile ad-hoc networks,” In Proc. IEEE ICNP, pages 251–260, 2001.

[4] J.-P. HuBaux, L. Buttyan, and S. Capkun., “The quest for security in mobile ad hoc network,” In Proc. ACM MOBICOM, Oct. 2001.

[5] L. Zhou and Z. J. Haas, “Securing Ad Hoc Networks,” IEEE Network, vol. 13, no. 6, pp. 24–30, 1999.

[6] P. Michiardi, R. Molva, “Ad hoc networks security,” IEEE Press Wiley, New York, 2003.

[7] P. Papadimitratos and Z. J. Haas, “Secure Routing for Mobile Ad hoc Networks,” in SCS Communication Conference (CNDS 2002), San Antonio, TX, Jan. 2002

[8] P. Papadimitratos, Z. J. Haas, & P. Samar, “The Secure Routing Protocol (SRP) for Ad Hoc Networks,” Dec. 02.

[9] Perrig, R. Canetti, J. Tygar, and D. Song, “The TESLA Broadcast Authentication Protocol,”Internet Draft, 2000.

[10] R. Ramanathan, J. Redi and BBN Technologies, “A brief overview of ad hoc networks: challenges and directions,” IEEE Communication Magazine, May 2002, Volume: 40, page(s): 20-22, ISSN: 0163-6804

[11] Y. -C. Hu, D. B. Johnson and A. Perrig, “SEAD: Secure Efficient Distance Vector Routing for Mobile Ad Hoc Networks”, Fourth IEEE Workshop on Mobile Computing and Applications (WMCSA’02), Jun. 2002.

Author Biographies

C.P. Agrawal has obtained B.E from College of Engineering, Amravati and M.Tech Degree from IIT, Kharagpur. He is working as Professor in Makhanlal Chaturvedi National University of Journalism and Communication, Bhopal. He has teaching and administrative experience of more than 20 years at national & foreign institutes. He has published more than 10 research publications. His area of interest is Wireless Communications.

Dr. O.P. Vyas has received his M.Tech. & Ph.D. degrees from IIT, Kharagpur. Presently he is working as Professor in Indian Institute of Information Technology, Allahabad. He has more than 25 years of rich Academic experience including 2 years in Europe as a DAAD Research Fellow in Germany and 03 months at CICC Japan. He has authored 3 books and published more than 60 research papers. His areas of interest include Wireless Networking and Data Ware Housing / Mining.

P. Udayakumar is a Reader in MCA department, Rungta College of Engineering and Technology, Bhilai (C.G) and member board of studies of Computer Applications, CSVTU, Bhilai. He has got MCA, M.Phil, and M.Tech(Hons.). His area of interest are wireless mobile communications, Artificial Intelligent and Computer Networks. He has authored a text book “Data Communication and Networks” through Sura Publications, Chennai. He has published about 12 papers in National International Conferences/ Journals.