A Review on various Security Attacks in Mobile Adhoc Network

Pritpal kaur[1], Er. Gaurav kumar[2]

M.Tech,CSE,Global Institute Of Management and Emerging Technology,Punjab,India
Professor, CSE,Global Institute Of Management and Emerging Technology,Punjab,India

---

ABSTRACT: Mobile Ad-hoc Networks or MANETs are largely found in things wherever any fixed facilities are simply not obtainable. MANET provides some basic responsibilities like routing, packet forwarding communication and network management etc. over self-structured network. This specially affects the energy, bandwidth and memory computation necessities. Providing trust in MANET is a further vital task because of lack of centralized infrastructure. Since throughout the deployment of but due to various types of intrusion threats and attacks it is hard to completely scrutinize any new node so as to allow only safe nodes to get connected with the prevailing safe system. The various attacks are discussed.

KEYWORDS:MANET, Security Attacks

1. INTRODUCTION:

We are moving from the old-style wired infrastructures to wireless communications. Wireless networks encompass variety of nodes that connect with one another over a wireless channel. Now-a-days in wireless devices, Mobile Ad-hoc Network become a very important half for communication for mobile devices. Self-configuring, freelance and decentralized while not having fastened hard and fast set infrastructure this of Network is thought as Mobile accidental Network. Mobile means the moving and accidental means that temporary with none fastened infrastructure so mobile accidental networks are a form of temporary networks during which nodes are moving with none fixed infrastructure. These networks don't have any fastened access points whereas each node may well be host or router. All nodes are capable of movement and might be connected dynamically in original manner.

1.1 CHARACTERISTICOF MANET:

1.MANET is capable of mult ihop routing.
2.Nodes will be part of or leave the network any time, it build configuration dynamic in nature.
3.InMANET,mobile nodes area unit characterized with less cash, power and light weight feature.
4.It has high density quality for variety of users.
5.It has strong and low price network.

2.SECURITY ATTACKS IN MANETS:

1. Passive attacks: A passive attack does not alter the information transferred in the network. But it includes the illegal "listening" to the network traffic or collects data from it.

2. Active Attacks: Active attacks are very simple attacks on the system that stop message movement between the nodes. These attacks produce illegal access to network that helps the attacker to make modifications such as alteration of packets, DOS, crowding etc.

3.Dropping Attacks: Cooperated nodes or selfish nodes can drop all packets that are not designed for them.

4.Modification Attacks: These attacks alter packets and disturb the whole message between system nodes. Sinkhole attacks are the example of alteration attacks.

2.1ATTACKS AT PHYSICAL LAYER:

1. **Eavesdropping:** Eaves dropping may be outlined as interception and reading of messages and conversations by careless receivers. The most aim of such attacks is to get the direction that must near be complete secret throughout the communication. The data might hold non-public key, public key, location or passwords of the nodes.

2. **Jamming:** Electronic counter measures could be a special category of DOS attacks that are initiated by malicious node once deciding the frequency of communication. During this sort of attack, the sender transmits signals together with security threats. Electronic countermeasures attack additionally prevents the reception of legitimate packets.

2.2 ATTACKS AT DATA LINK LAYER:

1. **Selfish Misbehaviour of Nodes:** Attacks below this category, are openly disturbs the self-performance of nodes and does not affect with the process of the network. It may contain two main factors.

- Preservation of battery power
- Fastpartialpart of bandwidth

2. **Traffic Analysis:** Traffic analysis can also be lead as active attack by finishing nodes, which encourages self-organization in the network, and valued data about the topology can be gathered. Traffic analysis in ad hoc networks may tell following type of information.

- Position of nodes
- System topology used for communication
- Characters played by nodes
- Existing source an endpoint nodes

3. COMPARISION OF ROUTING PROTOCOLS:

QUALITATIVE METRICES	**PROACTIVE**		**REACTIVE**		**HYBRID**	
	DSDV	**OLSR**	**AODV**	**DSR**	**ZRP**	**GPSR**
Loop free	Yes	Yes	Yes	Yes	Yes	Yes
Behavior	Proactive	Proactive	Reactive	Reactive	Combined proactive and reactive	Combined proactive and reactive
Security	No	No	No	No	No	No
Support for unidirectional links	No	Yes	No	No	No	No
Sleep mode	No	Yes	No	No	Partly	No
Multicasting	No	No	Yes	No	Partly	No
Routing	Flat	Flat	Flat	Flat	Flat and hierarchical	Flat
Nodes with special tasks	No	Yes	No	No	No	No
Routing Metrics	Shortest distance	Shortest distance	Shortest path	Shortest path	Shortest path	Shortest path

4. ATTACKS AT THE ROUTING LEVEL IN MANET:

ROUTING ATTACKS IN MANET	**ATTACKPROCEDURE**
Black hole Attack	Malicious node advertises itself as having a valid route and then consumes the intercepted packets.
Redirection with modified hop	Modifies hop count field in route discovery messages, determine shortest path

count	
Replay Attack	Records old valid Control message resends them to make other nodes update their routing tables with stale routes.
Wormhole Attack	Records traffic from one region of the network and replays it in different region
Rushing Attack	If the Route Requests that first reach the target's neighbors are those of the attacker, then any discovered route includes the attacker.
Message Bombing	By saturating the medium with a storm of broadcast messages
Shrew Attack	By sending short bursts repeated with a slow timescale frequency
Jellyfish Attack	Three Mechanisms: (a) Node delivers all received packets in scrambled order instead of the canonical FIFO order. (b) Same as that in the shrew attack, involves performing a selective black hole attack by dropping all packets for a very short duration at every RTO. (c) Holds received packet for a random time before processing it, increases delay variance.
	Alters MAC or IP address.
Falsifying Route Error Message	If destination node or an intermediate node along an active path moves, node also invalidates the route for this destination in its routing table, then by sending false route error messages.
Route cache poisoning	When information stored in routing table at routers is deleted, altered or injected with false information.
Routing Table Overflow	Attacker attempts to create route to non-existent nodes, prevents new routes from being created or Overwhelm the protocol.

5.CURRENT SECURE ROUTING PROTOCOLS:

Procedure of secure routing plays a very vital role in MANET's security. Due to fast increasing demand in mobile ad hoc networks the requirement for secure routing protocols becomes necessary so that the different security attacks can be prevent. Different present secure routing protocols with their benefits and drawbacks along with a comparison table.

1. SEAD: It stands for Secure Efficient Ad hoc Distance Vector Routing Protocol. SEAD is a proactive secure routing protocol based on DSDV routing protocol. It depends on one way hash chain of security to protector against Denial of Service. The idea after SEAD is to verify the sequence no. and metric of a routing table inform message using hash chain functions. Extended existed routing loops can be condensed by using endpoint sequence numbers which deliver replay protection of routing informs messages in SEAD.

Advantages: It is strong against many ungraceful attackers, cooperated nodes or energetic attackers. It plays important role in calculation and bandwidth-constrained nodes by using efficient, low-cost cryptographic primitives.

Disadvantages: It cannot validate smaller sequence numbers and it doesn't deliver a way to stop an attacker from damaging with "next hop" or "destination" columns.

2. SAODV: This protocol is measured to secure AODV. To use safety feature like verification and integrity SAODV is an improvement over AODV. To validate non variable fields messages such as route request (RREQ) and route reply (RREP) it uses digital signatures and to secure hop count data it uses hash chains. IP sec delivers safe data messages in communication in MANETs. Digital Signature is used when RREQ is sent from the source node to the destination node, sender signs the message. Middle nodes check the signature before generating or informing a reverse route. And only if the signature is confirmed they store the reverse route at last the destination node signs the RREP with its private key.

Advantages: Replay, delay attacks can be banned by sequence number system. Decreasing the hop count to increase the chance of being in the route path this can be stopped by using one way hash chain for hop authentication.

Disadvantages: Hateful node can pass the expected authenticator and hop count without changing them. Public key cryptography executes high processing overhead.

1. ARAN:ARAN is an on demand secure routing protocol and it depends on digital certificates. It offersauthentication, message integrity and non-denial .ARAN guarantee that each node knows the right next hop on a route to the destination by public key cryptography. During message transfer between source and destination it provides end to end guarantee.

Advantages: ARAN is talented of protective itself against spoofing, modification, fabrication, Denial of service attacks.

Disadvantages: It indications to wastage of bandwidth. It needs extra memory, has high processing overhead for encryption. Because it doesn't use hop count, so the discovered path
may not be optimal.

2. ARIADNE:A secure delay of DSR is Ariadne. It usages one way Message Authentication Code key chain TESLA. TESLA is capable authentication scheme that needs loose time synchronization. Araidne accept that the system links are bidirectional and network may drop, reorganize and replacement packets. In it each node must be able to guess the end to end estimation time to any other node in the network. Firstly it confirms route authenticity and secondly it checks that no node is missing on RREQ message .It uses one of the three schemes for authenticate routing messages: (a) Shared secrets between each pair of nodes. (b) Shared secrets between communicating nodes combined with digital signatures, or broadcast
authentication.

Advantages: It stops many types of DOS attacks. In it any alteration of node list can be
noticed and it stops attackers with uncompromised routes.

Disadvantages: It cannot protect against active attacks. Second the key exchange is very
complicated.

3. SLSP: It stands for Secure Link State Protocol . It known as individual and self-controlled link state detection protocol. SLSP is responsible for securing the route finding and transfer of link state information. It allocates safe proactive topology discovery which is useful for network operation. In this protocol every node is expected to be equipped with public/private key pairs and single network boundary per node within the Mobile Ad hoc Networks domain. Each node informs its neighborhood by neighbor lookup protocol and at times floods connection state inform packets to increase link state information.

Advantages: SLSP is strong against DOS and Byzantine attacks. Nodes can make a conclusion if they want to authenticate the public key or not.

Disadvantages: It is still weak to planning attacks.

4. SRP: It stands for Secure Routing protocol and it is on request routing protocol. Basic idea after this secure protocol is to form a security link between the source and destination with single notion that at the creation all nodes share a group key K and can be trusted. After that the key can be used to encrypt and decrypt the messages. This algorithm is appropriate for various applications like military and emergency situations.

Advantages: It guarantees the discovery of right connectivity information over an unknown network. Confidentiality is protected in presence of malicious node. Alteration of messages cannot be possible. Routing loops cannot be formed through malicious actions. Route signaling cannot be spoofed. Fabricated routing messages cannot be injected into network.

Disadvantages: It exposes network configuration with unencrypted routing path. Vulnerable to invisible node attack.

5. SAR:SAR uses AODV or DSR as a base protocol. To take safe and capable routing result this protocol studies trust level mechanism. It inserts the security metric into RREQ packet itself and changes the forwarding behaviour of the protocol. As middle nodes receive RREQ packet with a security metric or trust level the node can only process the packet or forward it if it can deliver the required security or trust level.

Advantages: To increase the significance of routes discovered by ad hoc routing protocols it allows the use of security as a open metric. SAR increase overhead due to calculations of encryption and decryption at each node.

Disadvantages: It doesn't describe anything about how to implement the security level as a
metric. Route discovery can be fail due to not having proper security clearance.

5.1COMPARI SION OF SECURE ROUTING PROTOCOLS:

PROTOCOLS	SECRET KEY	MAC	DIGITAL SIGNATURE	HASH CHAIN	CRYPTOGRAPHY MECHANISM	ASSUMPTION	VERIFICATION MECHANISM
SEAD	Initial secret key K for hash functions	----------	----------	One way hash func.to authenticate the Sequence no.	----------	Secure way of delivering initial secret key K	Hash chain verification
SAODV	Public/private key pair for each node	Used by sender	----------	One way hash func.to authenticate to hop counts	----------	Key distribution network	Digital signature verification mechanism
ARAN	Public/private key pair for each node		----------	----------	Public key cryptography	Trusted certificate server	Public key cryptography verification mechanism
ARIADNE	MAC keys ksd between sender and receiver	MAC ksd	----------	TESLA	----------	Nodes have loosely synchronized clocks	MAC verification mechanism
SLSP	Public/private key pair for each node	MAC	----------	----------	Threshold cryptography	Single network interface per node	Threshold Cryptography for key auntication, MAC verification
SRP	SA between Source and destination	MAC calculation	----------	----------	----------	Secure way of delivering the SA	MAC verification mechanism
SAR	Symmetric key encryption	----------	----------	----------	Simple encryption and decryption on each node	Shared key distribution network	Trusted level mechanism

RELATED WORK

Ajay Kushwaha et al. introduce a selective encryption method named Selective significantdata encryption (SSDE) for text data encryption. The SSDE provides sufficient uncertainty to the data encryption process as it selects only significant data out of the whole message. This in turn reduces the encryption time overhead and enhances the performance. The encryption part is performed by the help of symmetric key algorithm.

Shyam Nandan Kumar et al. present various schemes which are used in cryptography for Network security purpose. Network security covers the use of cryptographic algorithms in network protocols and network applications. They briefly introduce the concept of computer security, focuses on the threats of computer network security.

Alex Hinds et al.investigate the range of MANET routing protocols available and discuss the functionalities of several ranging from early protocols such as DSDV to more advanced such as MAODV.Some of the issues with MANET and the

AODV protocol in particular which were identified such as; power aware routing, Mobility aware routing, hierarchical routing, and reliability focused routing.

Saikumar Mankuet al. introduced Blowfish encryption algorithm for information security is designed and analyzed. The work is done for networking and communication application for enhanced network security. Blowfish algorithm reduces rounds of algorithm and proposed single blowfish round. Here the algorithm is modified so it provides great security thus no one in between sender and receiver will hack the data.

Priyanka Sharma et al. present a survey of the main types of attack at the network layer.
B.Nithya et al. present that day to day improving internet technology needs more and fast security for the communication channel, through which the information is passing. Even many algorithms are there to provide security to the network, almost of authors have studied and compared repeatedly the symmetric algorithms. This shows that symmetric algorithms have fastest than asymmetric algorithms.

CONCLUSION

Since MANETs have dynamic infrastructure and no centralized management they'reveryvulnerable to many varieties of attack. In this paper, we 'vem entioned Trust, Security challenges and differing kinds of attacks in Manet. Different security mechanisms are compared so as to check their effectiveness in handling network issues. Most previous and recent ad hoc networks have already targeted on providing routing services without considering any high level security.

REFERENCES

[1] B.Nithya,Dr.P.Sripriya" A Review of cryptographic Algorithms in Network Security" International Journal of Engineering and Technology (IJET) Vol 8 No 1 Feb-Mar 2016
[2] Nikunjkuar Varnagar,Prof.Amit Lathigara" Review Paper of Selfish Node Detection in MANET"InternationalJournal of Advance Research inComputer Science and Management StudiesVolume 3, Issue 2, February 2015
[3] Mr. Rahul Rajaram Kandekar, Prof. Amol A. Phatak"A Review Of Computer And Network Security" International Journal Of Innovations In Engineering Research and Technology [ijiert] issn: 2394-3696 volume 2, issue 5, may-2015
[4] Swati Kashyap, Er. Neeraj Madan" A Review on: Network Security and Cryptographic Algorithm"International Journal of Advanced Research in Computer Science and Software EngineeringVolume 5, Issue 4, April 2015
[5] Ms. Amruta Kodole, Prof. P. M. Agarkar" A Survey Of Routing Protocols In Mobile Ad Hoc Networks"Multidisciplinary Journal of Research in Engineering and Technology, Volume 2, Issue 1,2015
[6] Shyam Nandan Kumar"Review on Network Security and Cryptography"International Transaction of Electrical and Computer Engineers System, 2015, Vol. 3, No. 1, 1-11
[7]Deepti Ranaut, Madal Lal ''A Review on Security Issues and Encryption Algorithms in Mobile Ad-hoc Network" International Journal of Science and Research (IJSR) Volume 3 Issue 6, June 2014
[8] Priyanka Sharma, Dr. Surjeet Dalal" Reviewing MANET Network Security Threats" Priyanka Sharma al. International Journal of Recent Research Aspects, ISSN: 2349-7688, Vol. 1, Issue 2, Sept. 2014
[9] Jagtar Singh, Natasha Dhiman" A Review Paper on Introduction to Mobile Adhoc Networks" International Journal of Latest Trends in Engineering and Technology (IJLTET) ISSN: 2278-621X Vol. 2 Issue 4 July 2013
[10] Alex Hinds, Michael Ngulube" A Review of Routing Protocols for Mobile Ad-Hoc Networks (MANET)" International Journal of Information and Education Technology, Vol. 3, No. 1, February 2013
[11] Gagandeep, Aashima, Pawan Kumar"Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012
[12] Ankita Gupta, sanjay prakash ranga"various routing attacks in mobile ad-hoc
networks" volume 2 issue 4 july 2012
[13] kaur sharndeep, gupta anuj" a review on different secure routing protocolsand security attacks in mobile adhoc networks" int j adv engg tech/vol. v/issue iv/oct.-dec.,2014/01-05