IJCTA, 9(12), 2016, pp. 5703-5709

Trust Based Routing Methods to Pacify Network Layer Attacks in Mobile Ad-Hoc Networks–Survey

***S.Sargunavathi **J.Martin Leo Manickam Member IEEE**

Abstract : Mobile Ad-hoc Network (MANET) is an active Wireless Network of mobile devices that has been formed without any infrastructure. In MANET, each node acts as a router. Since it is vulnerable to security attacks, it can be easily accessed by any unauthorized network. If an unauthorized node in a network tries to access the MANET, there is a possibility of an attack. Several protocols have been proposed such as AODV, DSR to mollify the effects of routing behavior. One of the main challenges of MANET is to protect from various attacks. Several approaches have been proposed such as cryptographic and trust approaches. In this paper, we describe the performance of the protocol in cryptographic approaches and we present a detailed survey on trust based routing approach.

Keywords : Security Attack, MANET, Routing protocol.

1. INTRODUCTION

Mobile Ad-hoc Network (MANET) is a group of nodes which are not stationary *i.e.*(mobile), in which each node can be equipped with wireless Communication device.The transmission of mobile node is received by all the other nodes within its transmission range due to the nature of the wireless communication and Omni-directional antenna. If the sender node & receiver node are not within the transmission range (line of sight – direct), then an intermediate node between them are used to forward the messages.

2. SECURITY CHALLENGES IN MANET

The weak security causes the following :

1. **Easier to Tap :** Since the medium is air, the messages can be easily tapped in wireless communication.
2. **Limited Capacity :** It requires efficient Schemes with lesscontrol overhead.
3. **Dynamic Nature :** Due to the dynamic nature of mobile host, the self –organizing and self- forming algorithms are required to handle all types of attacks in MANET.
4. **Attack Susceptibility :** The wireless medium is more susceptible to jamming and other denial of service attacks.

A. Issues in MANET

The major issues in MANET are routing, Multicasting/broadcasting, location service, clustering, mobility Management, TCP/UDP, IP Addressing, bandwidth management, power management, security, fault tolerance, Quality of service, multimedia and standards/products. At present, routing, power management, bandwidth management, radio interface and security are the hot topics in MANET research.

* Pursuing Ph.D in Anna University, Chennai, India

** Professor in the department of ECE in St Joseph's College Of Engineering Chennai, India.

B. Applications of MANET

1. Battle field communication
2. Emergency self-scenarios
3. Law Enforcementü
4. Virtual Classroom
5. Public Meeting

Some of the attacks are listed below :

Table 1. Layers and their attacks

Sl.No	*Layer*	*Attack*
1.	Application layer	Repudiation, Data Corruption
2.	Transport layer	Session hijacking,SYN floodingWorm hole
3	Network layer	Worm hole, Blackhole, Byzantine, Grey Hole, resource consumption, Location disclosure
4	Data link layer	Traffic Analysis, Monitoring,Disruption, WEPweakness
5	Physical layer	JammingInterruption, Eavesdropping
6	Multi -layer	Denial of service, Impersonation, Replay, Man in Middle Attack

C. Goals of Security Attacks

Authentication, confidentiality, Integrity, Non repudiation, access control & availability to the mobile users or mobile nodes are the goals of security attacks in MANET.

D. Attacks in MANET

The MANET security is categorized in five layers. In MANET, attacks are divided into ***active attacks and passive attacks.***

Active attack : It attempts to modify or collapse the data being exchanged in the network, thereby conspiring the normal functioning of the network. It can also befurther classified into two categories such as external attacks and internal attacks.

Passive attack : It does not disrupt proper operation of the network. The attacker explores the data exchanged in the network without altering it. Here, the requirement of confidentiality can be violated since the operation of the network itself does not get affected, detection of passive attacks is very complex. One way of preventing such problems is to use advanced encryption mechanisms to encrypt the data being transmitted, thereby making it difficult for eavesdroppers to obtain any useful information from the data overhead.

3. ROUTING PROTOCOLS IN MANET

The protocols are classified into proactive (table driven), reactive(on demand)routing protocols.

A. Proactive protocols

It maintains table and it was updated periodically by every node in the network. E.g are WRP(Wireless Routing protocol), DSDV(Destination Sequenced Distance Vector)Routing Protocol and CGSR (Cluster Head Gateway) Switch Routing Protocol.

B. On Demand Driven/ Reactive Routing Protocol

On-Demand routing protocols execute the path detecting process and exchange routing messages onlywhen a path is needed by a node to communicate with a destination.

B.1. Dynamic source routing protocol

DSR is designed to restrict the bandwidth consumed by control packets in an ad-hoc wireless network. It is beacon less and therefore it does not require periodic packet (beacon) transmissions. During the route construction phase, it creates the route by flooding route request Packets in the network.Route request has a sequence number generated by the source node and the path is travelled. A destination node after receiving the first route request packet shows its response to the source node through the reverse path. A route reply is generated by when route reaches either the destination itself or an transitional node which contains in its route to the destination Flooding of packets consume asignificant amount of bandwidth in the already bandwidth- constrained network which increases the path setup time.

B.2. Ad-hoc On Demand Distance Vector Routing Protocol

AODV is a collective protocol and allows nodes to share the information they have about the remaining nodes in the network. During the route discovery RREQ messages arenot essential to reach the destination, if an intermediate node already knows the route towards the destination, it generates route reply RREP Message and does not forward the RREQ any further.This enables faster replies and controls the flooding of packets. AODV uses sequence number to identify fresher routing information. Each node has its own sequence number incrementing it before sending RREQ or RREP message. This sequence number is included in the routing table along with the routing message. AODV provides new information, thus nodes update their routing table, and if they receive the message with a sequence number greater than the previously recorded one for that destination. AODV does not give node's complete topology. Each node and itsneighboring nodes know the next hop to reach them.

4. CLASSIFICATION OF NODE MISBEHAVIOUR

There are no specific classes of node misbehavior, the best way to identify the classes of node misbehavior are as follows:

1. **Cooperative nodes,** which comply with the standard, at all times.
2. **Inactive nodes,** which include lazy nodes (unintentionally mis-configured) and constrained nodes (*e.g.* energy-constraint or field-strength-constraint).
3. **Selfish nodes,** which optimize their own profit, with neglect for the benefit of other nodes.

5. OBJECTIVE OF THE ROUTING APPROACH

There are two main broad routing approaches :

1. Cryptographic Approach 2. Trust based Approach

A. An Overview of cryptographic approach

Cryptographic schemes, like encryption and digital signature can defend external attacks. An another threat rises from compromised nodes, which sends false routing information to other nodes. Typical attacks in this category are black hole attacks, routing table overflow attacks, impersonation and information disclosure, etc. The internal attacks from malicious nodes are more severe because it is very difficult to detect due to compromised nodes and it can also generate valid signature. Existing routing protocols works better with the dynamic topology, but does not provide security measures.

This mechanism require a key management service. It helps to track key, node binding and assist the establishment of mutual authentication between communication nodes. Fundamentally, key management service is based on a trusted entity called CA and it issues public key certificate for every node. The trusted CA is required to be online. But it is dangerous to set up a key management service using a single CA in an ad hoc network. If CA is compromised, the security of the entire network is destroyed. A Threshold cryptography is used to provide robust and ubiquitous security support for the ad- hoc networks. The CA functions are distributed via threshold secret sharing mechanism. Using this black hole, grey hole, worm hole attack can be detected and

prevented. Most of the cryptographic approach is based on Public key Crypto systems (PKC) to achieve anonymity and unlink ability in routing. Inspite of Asymmetry PKC can offer best support in terms of privacy protection, Expensive PKC operations causes significant computation overhead.

ANODR (Anonymous On Demand Routing with untraceable router for Mobile Ad-hoc network) is based on PKC, it uses one time public/private key pair to achieve anonymity and unlink ability, but it cannot consider unobservability of routing messages During the route discovery process, each intermediate node create a onetime public/private key pair to encrypt/decrypt the routing so as to break the linkage between incoming packets and corresponding outgoing packets. Here the packets are publicly labeled and an attacker is able to distinguish different packet types, which fails to guaranteeun-observability.

ASR (Anonymous secure routing in mobile ad-hoc networks), ARM(A NONDSR Effective Anonymous Dynamic Source Routing For Mobile ad-hoc networks and ARMR(Anonymous routing protocol with multiple routes for communication in mobile ad-hoc networks are some of the protocols that also uses a onetime public key pairs to achieve anonymity and unlink ability.**ASR** is designed to achieve stronger privacy than **ANODR**

ARM (Anonymous Routing Protocol for Mobile Ad-hoc Networks) is considered to decrease the computation overhead on one time public/private key pair for privacy protection. **ARMR** uses the bloom filter along with keys to establish multiple routes for MANETS

SDAR (Secured Distributed Anonymous routing protocol for wireless and Mobile Ad hoc Networks) utilizes long term public/private Key pairs at each node for anonymous communication. ***SDAR***, ***ODAR*** are the advantages of network scalability, but they requires more computation effort. ***SDAR*** is similar to ARM except, that ARM uses shared secrets between source and destination for verification. UDAR offers anonymity but not unlinkability since RREQ\RREP packets are not protected with session keys.

J.Rey & Y.Li ,T.Li offered a solution for protecting privacy for a group of interconnected MANETS, but it has also the same problem of unlink ability. Mask is a special scheme based on pairing based cryptosystem, it also achieves anonymous concentration. It requires a trusted authority to generate sufficient pairs of secret points and corresponding pseudonyms as well as cryptographic parameters. MASK is quite expensive as it is vulnerable to key power depletion attacks. The RREQ flag is not protected, this enables passive adversary to locate the source node.

An **ALARM(Anonymous Location Aided Routing in suspicious MANETS):**It uses public key cryptography and group signature to preserve privacy.The group signature is good in privacy preserving feature and everynode can verify a group signature. But it cannot identify who is the signature of privacy information.

USOR (Unobservable Secure On demand Routing protocol for Mobile Ad-Hoc networks)is anunobservable routing scheme . In this routing protocol, only a valid node can identify the routing packets with inexpensive symmetric decryption. The intuition behind the USOR scheme is that if a node can establish a key with each of its neighbor, then it can use such a key to encrypt the whole packet for a corresponding neighbor. The receiving neighbor can identify whether the encrypted packet is intended for itself by trial decryption. AODV is not designed with malicious nodes. More subsequent extension type of protocols had been proposed. Many of these extension protocolsuse the cryptographic methods to the existing protocols to route the packet securely. It is observed that such approach prevent interference with the routing information, but a DOS attack is established .This type of attack is effective in MANET devices with limited battery power and limited computational power and also allows the attacker to shut down the nodes. USOR is based on group signature and id based cryptosystems for ad-hoc networks. It offers strong privacy protection, complete unlink ability and the content observability for ad-hoc network. It also provides more resistant against attacks due to node compromise. But, by varying this scheme wormhole, DOS cannot be prevented.

B. Objective of trust based protocols

The objectives of the trust based protocols are :

1. Light weight
2. Cooperative
3. Attack tolerant
4. Flexible
5. Compatible
6. Scalable

C. Overview of the Trust Approach

It describes the trust approach in MANETS.

C.1. Trust Prediction and Diagnosis

If one network entity establishes trust in another network entity it can predict the future behavior of other networks and diagnose their security properties.This forecast diagnosis can solve or partially solve the following:

1. Providing Assistance in decision making to improve security and robustness.
2. Risk Adaptation which in turn leads to flexible security solution.
3. Misbehavior detection.
4. System level Quantitative assessment in security properties.

The trust is classified as direct trust and indirect trust.

C.2. Direct trust

It is established through observations and checks whether the previous interactions between subject (first party) and the agent (second party) are successful or not.

C.3. Indirect Trust

Trust can transit through third parties.eg If X trust Y, Y trust A, X can trust A to a certain degree if Y Tells X its trust opinion (RECOMMENDATION) of A. This Phenomenon is called trust propagation.

Integrating trust in a distributed network gives the advantage of detecting malicious node, defeats bad mouthing attack, on-off attack, conflicting misbehavior attack.

Further, the trust models are classified into two types namely independent model, cross model.

1. **Independent model** represents independent ad-hoc networks without any connection to the fixed network.
2. **Cross model** represents ad-hoc networks with few connections to the fixed networks.

In both the models, the basic unit is a personal trusted bubble (PTB). In the bubble, the owner of the ad- hoc device irrationally trusts fully on the device. Here, the trust evaluation mechanism is introduced in each PTB. The trust relationship between host bubble &other bubble is evaluated digitally according tothe knowledge of the bubble owner. Each bubble has a trust matrix, which stores the knowledge used for trust evaluation. There is one more method implemented in which the trust based evaluation system combined with on demand ad-hoc routing protocol with suitable modifications and by adding knowledge accumulation system, the protocol is analyzed for black hole attacks, denial of service attack, routing table overflow attacks and energy consumption.

A trust model is derived based on the history of direct interactions among nodes to compute trust.They use passive acknowledgement as the single observable factor for accessing the trust. This passive acknowledgement uses the promiscuous node to monitor neighbor'sbehavior in the wireless radio channel, which allows a node to detect any transmitted packet in its transmission range, irrespective of destination. It is very well known that, all packets in MANETS can be classified into control packets, data packets. Control packets are used for route request, route reply, route update, route error .The accuracy of control packets play the important role in establishment of accurate routes in the network. So the forwarding ratio is divided as control packet forwarding ration DFR(t).They are computed using forwarding count of control packets and data packets. Assigning the weight to CFR(t),DFR(t) is used to determine the overall trust values of a node. Trust values are updated based on trust update threshold.

Novel multipath reactive routing protocol (AOTDV) is proposed based on AODV to discover trust worthy forward paths and attenuate the attacks from maliciousnodes.In that protocol, source establishes a trustworthy path to the destination in a single route discovery. Route discovery is initiated only when all path breaks or fails to meet trust requirements of data packets. AOTDV is compared with AODV, AOMDV and shows improvement in packet delivery ratio and detect malicious nodes. But the forwarding ratio of more recent window is given as larger weight.Assigning a smaller value will make the above work more satisfactory.A trust based cross layer security protocol (TCLS) is developed which provides confidentiality,authentication of packets in both routing and link layers of MANETS. In TCLS protocol, during the first phase, trust based packet forwarding scheme is designed for detecting and isolating the malicious node. It uses a trust counter for each node. A node is punished and rewarded by incrementing and decrementing the trust counter.If the trust counter value falls below a threshold, the corresponding intermediate node is marked as malicious.TCLS achieves authentication using route reply operation.Nodes which is stored in the current route perform cryptographic computation. In the next phase, link layer security using CBC-X is used for authentication .TCLS achieves high packet delivery ratio with low overhead,low delay.

6 CONCLUSION AND FUTURE WORK

This article describes the related work of routing approaches. Each approach has its own merits and demerits. By using this survey, we planned to compose an optimized trust routing algorithm and to establish some fast response mechanisms when node behaviors such as attacks are detected. We will also work at applying the trust model into other applications (*e.g.*, key management) and other routing protocols of the MANET. Detailed simulation will be conducted in terms of message overhead, security analysis, packet delivery ratio and throughput.

7. REFERENCES

1. “Survey of attacks and counter measures in Mobile Ad- hoc networks”, y. Xiaoshen & D-2 Wireless/Mobile Network Security 2006 Springer.
2. “Ad-Hoc Wireless Networks Architectures and Protocols” ,C. Sivaram Murthy B.S. Manoj
3. “OSI layer computer networks”, Forouzan
4. On the impact of user profiles on the interoperability of Wi-Fi systems and cellular networks”. Technical support department of CSE,IIT Madras by D.A Joseph, B.S. Manoj, C.Sivarammurthy
5. ”Defense of Trust Management Vulnerabilities In Distributed Networks “,Yan Linsay sun university of Rhodeisland ,Zhu Han Boise State University,K.J. Ray Liu university of mary land Security in Mobile Ad-hoc and Sensor Networks. IEEE Magazines Feb 2008.
6. **“**Based On Demand Multipath Routing In Mobile Ad-Hoc Networks”, X.LiZ. JiaP. ZhengR,. ZhangH.Wing, IET Information Security 2010
7. **“**Trust Evaluation Based Security Solution In Ad-Hoc Networks”, ZhengYan, Peng Zhang Teemupekka Virtanen.
8. **“**Routing security in Wireless Ad-hoc networks**”**.IEEE Communication Magazine Hang mei Deng Wei li dharma P.Agarwal.
9. “Fuzzy based Trust Prediction Model for Routing in WSNs” X,Anitha M.A Bhagyaveni and J Martin Leo Manikam The Scientific World Journal July 2014.
10. “Path Tracing Based Metric Analysis Of Wormhole Detection” M.P.Manjunath, N.Priyanka, Lakshmi Kumar, Mr.M.Reji Mano, Dr.P.C.Kishore Raja, International Journal of Applied Engineering Research” (Ijaer), 2015.
11. “Mobile Ad Hoc Networking”, Stefano Basagni (Editor), Marco Conti (Editor), Silvia Giordano (Editor), Ivan Stojmenovic (Editor), ISBN: 978-0-471-65688-3.

12. "Cross Layer Detection of Wormhole In MANET Using FIS", P. Revathi, M. M. Sahana & Vydeki Dharmar, ITSI Transactions on Electrical and Electronics Engineering (ITSI-TEEE), 2013.

13. "Detecting and Avoiding Wormhole Attacks in Wireless Ad Hoc Networks", Farid Naït Abdesselam, Brahim Bensaou, Tarik Taleb,IEEE Communications Magazine.

14. "Secured Fuzzy Based Routing Framework for Dynamic Wireless Sensor Networks",I. Sakthidevi, E. Srievidhyajanani, International Conference on Circuits, Power and Computing Technologies, 2013.

15. "Fuzzy and cluster based SIP protocol for MANET", Almobaideen, W.Kubba, N.Awajan, Proceedings of International Conference on Next Generation Mobile Apps, Services and Technologies, pp. 169-174, IEEE 2014.

16. "A domain based multi-cluster SIP solution for mobile ad hoc network", Aburumman, A.Choo, K.K.R, Proceedings of International Conference on Security and Privacy in Communication Networks, Springer, 2015.

17. "Mobile Ad hoc Network Security – A taxonomy", S. Alampalayam, A. Kumar, S. Srinivasan, IEEE 2015.