A Survey of Secure Routing Protocols of Mobile AdHoc Network

S.Ranjithkumar[1], N. Thillaiarasu[2],

1 Department of Computer Science and Engineering / S N S College of Engineering / India
2 Department of Computer Science and Engineering / S N S College of Engineering / India

ABSTRACT — the mobile ad hoc network is a fast growing research due to their flexibility and independence of network infrastructure. It's a challenging task compared to conventional network because of its unique characteristics such as dynamic network topology, limited bandwidth and limited battery power. There are several efficient routing protocols have been proposed for MANET. These are efficient, but in the presence of malicious node there are vulnerable to various kinds of attacks. In this article, we compare the various routing protocols present in MANET and various attacks in the existing MANET protocols.

Keywords— *Routing Protocols; Malicious Node; node attack; Security; etc.*

I. INTRODUCTION

A MANET is self-configuring, infrastructure-less network for mobile services connected without wires. It varies from mesh network as it is self–forming, self-healing network. The main problem in the network is equipping each device to continuously maintain the information required to properly route traffic. The equipments operate by themselves or can be connected to the internet. This results in a highly dynamic, autonomous topology. The various routing algorithms in MANET are

- Dynamic Source Routing (DSR),
- Ad Hoc On-Demand Distance Vector Routing (AODV) and
- Destination Sequenced Distance-Vector (DSDV)

II. ROUTING ALGORITHMS

A. DSR PROTOCOL

The DSR is an on-demand routing protocol for wireless network, it relies on source routing instead of routing table at each intermediate nodes. To accomplish source routing, the routed packets contain the address of each device the packet will traverse, which result in high overhead for long paths or large addresses, like IPv6. To overcome this using source routing, the DSR optionally defines a flow id option that allows packets to be forwarded on a hop-by-hop basis.

It has 2 major phases, which are Route Discovery and Route Maintenance. Only after the message reaches the destination Route Reply will be generated. In case of erroneous transmission, the Rout maintenance Phase is initiated which initiates the Route Error packet generation. Then the erroneous hop will be removed from the nodes cache and new route will be again identified using Route Discovery Phase.

B. AODV PROTOCOL

In AODV, the network remains silent until the connection is needed. When the connection is needed, the needy node broadcasts a message to all the AODV nodes. The AODV node sends the temporary nodes back to the needy node. The needy node then begins to use the route that has least number of hops through other nodes. The unused entries present in the routing table are recycled. When there is a failure in the link, the routing error is passed back to the transmitting node. This process repeats. The main features of AODV are sequence number, time to live and route requests. The advantage of AODV is that it create4s no extra traffic for communication along existing links. But it requires more time when compared to DSR which is simple and does not require much memory or calculations.

C. DSDV PROTOCOL

DSDV (Destination-Sequenced Distance Vector RoutingDSDV) is a table driven routing scheme. Its based on Bellman-Ford algorithm. Each entry in the routing table contains a sequence number which is generated by the destination by the destination and the emitter needs to send out the next update using this number. Routing information is distributed between nodes by sending full dumps infrequently and smaller incremental updates more frequently.

III. Routing algorithms Comparisions

A. DPRAODV PROTOCOL[1]

DPRAODV was introduced to overcome the disadvantages of AODV. In case of AODV it does not lie on the active path, does not maintain any routing information and also does not participate in table exchanges periodically. To accomplish these DPRAODV introduces 2approaches namely the

- Secure Adhoc Routing
- Intrusion Detection.

1) *Secure Routing :*

Like the DSDV which uses hash chains to authenticate hop counts and sequence numbers ,Ariadne assumes the existence of a shared secret key between two nodes based on DSR. Cryptographic public-key certificates is used by a standalone protocol called the Authenticated Routing for Ad hoc network(ARAN).The security goals are achieved using Security –Aware Ad hoc Routing(SAR).It makes use of security attributes such as trust value and relationships.

2) *Intrusion Detection System[1] :*

It uses the Route Confirmation Request (CREQ) to next hop onwards the destination. The detection process is based on stable-based misuse detection system. The drawback is that overhead in routing increases causing performance degradation. The Black hole attack can be avoided using DPRAODV.

B. GRAY HOLE ATTACK[1]

The gray hole attack has 2 phases In the first phase, a malicious node exploits the AODV protocol to advertise itself as having a valid route to a destination node.

- In the phase 2, the node drops the intercepted packets with a certain probability.

The AODV can be used against the gray hole attack, which involves 4 security procedures.

- Neighborhood data collection,
- Local anomaly detection,
- Cooperative anomaly detection.
- Global alarm raiser.

1) *Neighborhood data collection module[2*

Each node in the network collects the data forwarding information in its neighborhood and stores it in a table known as the *Data Routing Information* (DRI) table. This identification is done on the basis of the nodes that have '0' entries both in the '*From*' and '*Through*' columns in the DRI table The 'RTS/CTS column in the DRI table gives the ratio of the number of *request to send* (RTS) messages to the number of *clear to send* (CTS) messages for the corresponding node.

2) *Local anomaly detection module[2]:*

Security procedure is invoked by a node when it identifies a suspicious node by examining DRI table. *Initiator Node* (IN**)** first chooses a *Cooperative Node* (CN**)** in its neighborhood based on its DRI records and broadcasts a RREQ message to its 1-hop neighbors requesting for a route to the CN.

- 1In reply to this RREQ message the IN will receive a no. of RREP messages from its neighboring nodes.
- It will undoubtedly receive a RREP message from the *Suspected Node* (SN) if the latter is really a gray hole

2) *Cooperative anomaly detection module[2]*

Objective is to increase the detection reliability by reducing the probability of false detection of local anomaly detection procedure. A gray hole will just change its phase from '**good' to 'bad'** immediately after the invocation of one round of the detection algorithm is over and will switch back to 'good' phase just before the next invocation.

3) *Global alarm raising module[2]:*

process is invoked to establish a network wide notification system for sending **alarm messages** to all the nodes in the network about the gray hole node(s) that has been detected by the cooperative anomaly detection algorithm.

C. *A Dynamic Anomaly Detection Scheme[5]*

- To enhance the security in MANETs
- an approach that requires the intermediate nodes to send a route reply (RREP) packet with the next hop information
- "Further Request" packet to the next hop to verify that it has a route to the intermediate node and a route to the destination.

- When the next hop receives a "Further Request" packet, it sends a "Further Reply" packet that includes the verified result to the source node.
- then it sends a route confirmation reply (CREP) message to the source node with its route information *Network Monitoring-Based Attack Detection*
- Network monitoring can detect attacks from inside MANETs,
- Network monitoring nodes are selected to collect all the packets within a cluster, and the decision agents in the nodes are used to detect and classify the security violations.
- AODV-based State Transition Analysis Technique (AODVSTAT) sensors placed within the network to detect attack.
- In addition, a large number of UPDATE messages may cause an overwhelming congestion in the network.

1) *Anomaly Detection[5] :*

*T*he packet flow is observed at each node and they constructed an extended finite-state automaton (EFSA) according to the specification of the AODV routing protocol

D. *ATTACKS ON AODV PROTOCOL[3]*

1) *Overview*

- At the start of communication routes are generated by Network
- Each and every node has its own sequence number, and this number increases whenever a link changes.
- Sends a route request (RREQ) message by using broadcasting. The RREQ ID increases by one every time node *S* sends an RREQ message
- If they have a valid route to the destination, then they send an RREP message to node.

2) *Classification of Attacks[5]*

a) *Routing Disruption Attacks:*

- Suspend the establishment of a route or destroy an existing route.
- Universal attacks of this type are the modification of RREP (same as the Black hole Attack) and the modification of RREQ.

b) *Resource Consumption Attack:*

- Attack wastes resources of a specific node and the network as a whole.
- Universal attack of this type is malicious flooding.

E. *Bootstrapping Security Associations for Routing[6]*

1) *A Cyclic Dependency Problem[6]:*

Routing service depends on security services to authenticate the source of a message (i.e., its IP address) and the message content.

To acquire secure bindings between a node's IP address and key, it must either reach a trusted-authority node or establish trust relationships with other nodes without relying on trusted authorities.

2) *Breaking the Cyclic Dependency[6]*

We remove dependency by using a *secure binding mechanism* for establishing secure node-to-node associations that is *independent* of secure routing and other security services. Idea of a secure binding between an IP address and a key that is independent of any other security services by control messages of MIPv6.

F. *Security Analysis of the protocol[6]*

1) **Attack1**

Node 1 receives a **route request** from source node S and tries to **send a reply** to S giving a false route.

2) *Attack 2*

Malicious nodes may try either to shorten or to lengthen a route by modifying the node list on a *Route Request.*

3) *Attack 3:*

Intermediate nodes, might modify a ***Route Reply*** (add to or delete from the node list), but S would not accept the modified *Route Reply* as a signature or the message authentication code of D would not pass S's authentication check.

4) *Attack 4:*

An attacker can flood a node with route requests and exhaust its resources as the node has to authenticate packet signatures, and signature authentication is a computationally intensive operation.

5) Attack 5:

An attacker might want to mount a replay attack. Replayed requests will be detected at D and replayed replies will be detected at S by using standard mechanisms based on sequence numbers.

G. Intrusion Detection[8]

The Optimized Link State Routing (OLSR) protocol is a proactive Mobile Ad hoc Network (MANET) routing protocol.

1) The OLSR Protocol[8]

A variation of the pure Link State Routing (LSR) protocol and is designed specifically for MANETs In comparison to LSR, the optimization in OLSR localizes parts of routing selection; while computing the routing table to a destination, only MPR nodes are considered as the last hops to the destination instead of all neighbor nodes to the destination; each node picks its own MPRs instead of making a routing calculation to decide which neighbors serve as the last hop to the destination.

This localization increases the threat to the security of the network routing but also provides advantages for local control message validation because of the intrinsic relationship between the HELLO message and the TC message.

2) OLSR Vulnerabilities [8]

a) MANET application environments such as the battlefield or law enforcement situations are exposed to more threats than other environments such as electronic classrooms.

b) Due to the open medium environment in a MANET, an intruder can join in the routing process without any attaching point.

c) Dynamic membership and topology due to mobility are also big holes for security.

3) Intrinsic properties of OLSR messages [8]

Property 1:

An HELLO message originating from a MANET node contains all one-hop neighbors of the node. A TC message originating from the same MANET node contains only MPRs selectors of the node. The TC set is always a subset of the hello set to the same MANET node.

Property 2:

If a MANET node receives a TC message that lists itself as an MPR selector, the originator of the TC message must be in the neighborhood of this MANET node. TCp represents the TC set originating from Node P, and HelloC represents the HELLO set of Node C.

Property 3:

If a MANET node receives a TC message originating from its neighbors and notices that the TC message lists itself as an MPR selector, this MANET node must have listed the TC originator as an MPR in its HELLO message first. Node P and Node Q are neighbors; T p represents the TC set originating from Node P; M q represents the MPR set in Node Q.

Property 4:

The sender of a TC message will hear the same TC messages that are forwarded by all its MPRs. The MPR nodes only change the source IP address in the IP header and keep the IP payload; the TC message is unchanged. T p represents the TC set sent from Node P; M1, M2, Mi …Mn represent all the MPR nodes of Node P.

H. PRISM: Privacy-friendly Routing in Suspicious MANETs (and VANETs) [9]

Mobile Ad-Hoc Networks (MANETs) play an increasingly important role in many environments and applications, especially, in critical settings that lack fixed network infrastructure, such as: emergency rescue, humanitarian aid, as well as military and law enforcement.

MANET deployment scenarios involve operation in *hostile* environments, meaning that attacks are either expected or, at least, possible. Moreover, threats can originate from both outside and inside the network.

Application Examples:

Military and law-enforcement MANETs are compelling examples of settings where privacy, in addition to security, is very important.

Zooming in on the military example, one can imagine a battlefield MANET composed of different types of nodes, like infantry soldiers, vehicles, and aircrafts as well as other types of personnel and equipment.

If the adversary can track nodes' movements, it can easily deduce node types. For example, one that moves 50 miles within 10 minutes is most likely, an aircraft. Whereas, one moving only 5 miles within the same interval is probably a vehicle.

1) *DESIGN ELEMENTS[9]*

a) *Goals*

Privacy: Exploit tracking-resistance of individual nodes, by outsider and insider adversaries.

Security: provide protection against active and passive outsider and insider attacks.

Efficiency: attain the above two goals with reasonably efficient solutions.

b) *Long-Term Identities Considered Harmful[9]*

The first threat comes from outsiders: tracking nodes based on their identifiers is possible by eavesdropping on routing information exchanged. This can be easily remedied by having all MANET nodes share a network-wide key and encrypting all routing information.

The second threat comes from malicious insiders, i.e., MANET nodes that aim to track their peers. This threat is much harder to address, since a typical (even secure) MANET routing protocol is designed to provide routing information based on a destination address.

c) *One-Time Pseudonyms[9]*

In a link-state based protocol such as OLSR, each node propagates its immediate neighborhood information to all other nodes. Thus, if each node has a collection of unrelated pseudonyms, it uses them, one at a time, to avoid being tracked. In a distance-vector protocol, such as DSDV, a node can also periodically switch to a new pseudonym and shed its previous identity.

d) *Communication Paradigm[9]*

Our privacy goal dictates that long-term identities can only be used in conjunction with flooding (which is inefficient). Whereas, random shortterm(one-time) identities are not meaningful as the sole basis for communication.

IV. CONCLUSION

A MANET is an emerging technology that has-been attracting tremendous attention from researchers. For the reason that these networks can be deployed quickly without relying on a predefined infrastructure and they can be applied in various situations ranging from emergency operations and disaster relief to military service and task forces. Obviously, providing security in such scenarios is critical. The main disadvantage of MANET is that it is resource constrained i.e limited bandwidth, battery power and computational power, and it lacks a reliable centralized administration. The technologies that are used for the wired network cannot be applied for the MANET.

The various routing protocols have been explained in this paper and their advantages and drawbacks have been identified. Though various solutions have been proposed still the attacks in MANET prevail. Some solutions may require special hardware such as a GPS or a modification to the existing protocol.

REFERENCE

[1] Klaus Pl oßl, Thomas Nowey, Christian Mletzko "Towards a Security Architecture for Vehicular Ad Hoc Networks" The First International Conference on Availability, Reliability and Security, 2006, pp. 374 ARES 2006.

[2] Xiaoqi Li, Michael R. Lyu, "A Trust Model Based Routing Protocol for Secure Ad Hoc Networks" IEEE Aerospace Conference, 2004.

[3] Mike Burmester, Breno de Medeiros "On the Security of Route Discovery in MANETs" IEEE Transactions on Mobile Computing, Issue No.09., vol.8., pp: 1180-1188 – September 2009.

[4] Payal N. Raj, Prashant B. Swadas B.V.M.Anand, "DPRAODV: a dynamic learning system against Black hole attack in AODV based MANET" IJCSI International Journal of Computer Science Issues, Vol. 2, 2009

[5] Hidehisa Nakayama, Satoshi Kurosawa, Abbas Jamalipour, Yoshiaki Nemoto, Nei Kato "A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks" IEEE Transactions on Vehicular Technology, vol. 58, no. 5, June 2009 2471.

[6] R.B.Bobba, L.Eschenauer, V.D.Gligor, W.Arbaugh "Bootstrapping Security Associations for Routing in Mobile Ad-Hoc Networks" IEEE Global Telecommunications Conference, 2003. GLOBECOM '03. pp. 1511 - 1515 vol.3

[7] Jaydip Sen, M. Girish Chandra, Harihara S.G., Harish Reddy, P. Balamuralidhar "A Mechanism for Detection of Gray Hole Attack inMobile Ad Hoc Networks" 6th International Conference on Information, Communications & Signal Processing, 2007. pp. 1 – 5.

[8] M. Wang, L. Lamont,Communications Research CentreP. Mason, M. Gorlatova, "An Effective Intrusion Detection Approach for OLSR MANET Protocol" 1st IEEE ICNP Workshop on Secure Network Protocols, 2005. (NPSec). pp. 55- 60.

[9] El Defrawy, K. Tsudik, G.PRISM: Privacy-friendly Routing In Suspicious MANETs (and VANETs) IEEE International Conference on Network Protocols, 2008. pp.258 – 267.

[10] Y-C Hu and A. Perrig, "A Survey of Secure Wireless AdHoc Routing," IEEE Sec. and Privacy, May–June 2004.

[11] K. Sanzgiriet al, "A Secure Routing Protocol for AdHoc Networks," IEEE International Conference on Network Protocols, Nov. 2002.

[12] Y-C. Hu, A. Perrig, and D. B. Johnson, “Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks,” Proc. Mobi Com ’02, Atlanta, GA, Sept. 23–28, 2002.

[13] M. G. Zapata and N. Asokan, “Securing Ad-Hoc RoutingProtocols,” ACM Wksp. Wireless Sec., Sept.2002, pp. 1–10.

[14] B. Wu et al., “A Survey of Attacks and Counter measures in Mobile Ad Hoc Networks” Wireless/Mobile Network Security, Springer, vol. 17, 2006.

[15] S. Marti et al., T. J, Giuli, Kevin Lai, Mary Baker “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,” 6th annual international conference on Mobile computing and networking, Pages 255-265