Review Paper on Enhancing Performance and Security of Routing Protocol on MANET

Pathan Sohel Alarakhbhai
PG Student
Computer Science&Engineering, S.P.B.Patel Engineering College, Mehsana, India
pioneerpathan@gmail.com

***Abstract*— several routing protocols have been proposed in recent last years for possible deployment of Mobile Ad hoc Networks (MANETs) in different area military, government and commercial applications. In this paper, we review these protocols with a particular focus on security aspects. The protocols differ in terms of routing strategies and the data used to make routing decisions. The analyses of the secure versions of the proposed protocols are discussed with respect to the above security requirements. We provide a survey on the present state of analysis techniques, as they are used in the mobile ad hoc routing community and further discuss open research areas. The Mobile Ad-hoc Network (MANET) is a collection of self-configuring mobile node without establishing any infrastructure. This is anticipated to offer an area of flexible services to mobile and nomadic users by means of integrated homogeneous architecture. The proper routing protocol is necessary for better communication in MANET. One of the existing reliable protocols is Ad Hoc On-Demand Vector Routing (AODV) protocol which is a reactive routing protocol for ad hoc and mobile networks that routes only between nodes that wants to communicate. SAODV is an extension of the AODV routing protocol that can be used to shield the route discovery process by providing security characteristics like integrity and authentication.**

***KeyWords* — Ad hoc networks, routing protocols, security, wireless systems, mobile routing, AODV protocol, SA-AODV protocol. *Index Terms*—Component, formatting, style, styling, insert.**

1. INTRODUCTION

In ad hoc network is usually defined as an infrastructure less network. This means that a network is lacking the standard routing infrastructure like fixed routers and routing backbones. Usually, the ad hoc nodes are mobile and the fundamental communication medium is wireless. Every ad hoc node possibly will be able to of act as a router. Such ad hoc networks may arise in personal area networking, meeting rooms and conferences, disaster relief and rescue operations, battlefield operations, etc. Routing in ad hoc networks has been an active research area and in recent years numerous routing protocols have been introduced for MANETs the topology of the ad hoc network depends on the transmission power of the nodes and the location of the mobile nodes, which may change with time.Protocol security is vital to proper operation. We consider a protocol secure if it is accurate and reliable, even when faced with malicious attackers. In order for a MANET routing protocol to operate properly, we must trust intermediate nodes that make up a routing path will operate according to the protocol rules. A wireless ad hoc network is primarily divided into two areas; Mobile Ad hoc Networks (MANET) and Smart Sensor Technology. Mobile ad hoc networks consist of mobile nodes, which can communicate with each other and nodes can enter and leave the network anytime. This dynamic nature brings in frequent topological changes in the network, making routing between mobile nodes a very difficult and challenging task. These challenges, along with the significance of routing protocols, make routing area the most active research area in the MANET domain.

2. ROUTING PROTOCOLS CLASSIFICATION IN BRIEF

Routing is the process of finding a path from a source to destination among randomly distributed routers. The broadcasting [7, 8, 9] is inevitable and a common operation in ad-hoc network. It consists of diffusing a message from a source node to all the nodes in the network.

Mobility: the network topology in an ad hoc wireless network is highly dynamic due to the movement of nodes and the addition of new nodes to the network. Disruption in service may occur either due to the movement of the intermediate nodes in The path or due to the movement of the end nodes. Broadcast can be used to diffuse information to the whole network. It is also used for route discovery protocols in ad-hoc networks. The routing protocols are classified as follows on the basis of the way the network information is obtained in these routing protocols.[4]

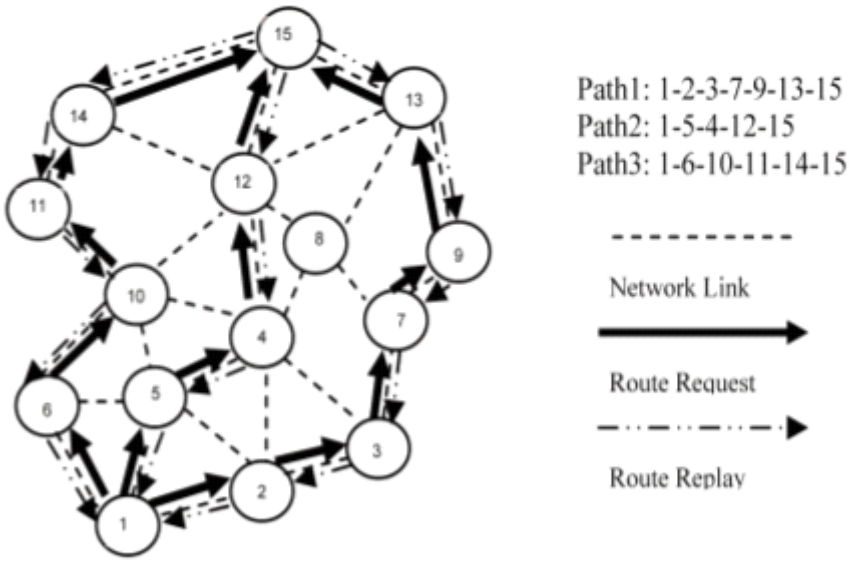

Figure.1 Routing in MANET [16]

2.1 Proactive (Or Table-Driven) Routing Protocol

The proactive protocols maintain routing information about each node in the network. The information is updated throughout the network periodically or when topology changes. Each node requires to store their routing information. For example

1. Destination sequenced Distance vector routing (DSDV)[10]
2. Source Tree Adaptive Routing (STAR)[11]

2.2 Reactive or On-demand routing protocol

The reactive routing protocols look for the routes and are created as and when required. When a source wants to send to a destination, it invokes the route discovery mechanisms to find the path to the destination.

For example

1. Ad-Hoc On-demand Distance Vector (AODV)[12]
2. Dynamic Source Routing (DSR)[13,14]
3. Dynamic MANET On-demand (DYMO)[15]

2.3 Hybrid Protocols

These protocols are using the best features of both the on-demand and table driven routing protocols. These classes of routing protocols are reported but choosing best out of them is very difficult as one may be performing well in one type of scenario the other may work in other type of scenario. In this paper it is observed with the simulation of AODV, DSR and STAR routing protocols [8].

3. LITERATURE SURVEY

As AODV lacks security mechanisms, malicious nodes can carry out several attacks just by not behaving based on the AODV rules. Therefore, to guarantee the entire security of the network, it is important to create security mechanisms that can withstand malicious attacks from insiders who have entire control of several nodes. For the purpose of protection against insider attacks, it is required to realize how an insider can attack a wireless ad-hoc network.

Various attacks have been discussed in various literatures. According to the composition of operations for carrying out attack as mentioned in above article, misuses of AODV have been divided into two categories: atomic misuses and compound misuses. Intuitively, atomic misuses are carrying out by controlling a single routing message that cannot be any more separable. On the contrary, compound misuses are composed of multiple atomic misuses, and possibly normal uses of the routing protocol. Initially, it is required to determine a number of misuse goals that an inside attacker may require to achieve and are listed as follows.

Researchers now have proposed several protocols to secure the AODV protocol. K. Sanzgiri and B. Dahill have developed authenticated routing for ad hoc networks on AODV (ARAN)[10]. In ARAN, very node has its digital certificate signed by a trusted authority. ARAN uses a digital signature to provide authentication of all unaltered information in Route Request and Reply packet. Each node along the route should check the signature of its upstream node and replace it with its own signature.

However, ARAN is not complete since it does not provide enough protection to hop_count information. M. Zapata and N. Asokan also proposed a secure AODV protocol (SAODV)[11]. Similar digital signature protection as ARAN is used in SAODV and it further use one-way hash chain to secure the hop_count information from being decreased. This idea is borrowed from SEAD[9]. However, the one-way hash chain can not stop any attackers or selfish nodes from increasing the hop_count or just keeping it unchanged.

Secure Routing with AODV (SRAODV), a series of security mechanisms, including Key Exchange, Secure Routing, Data Protection, are proposed by A. Pirzada and C. McDonald[12]. Considering about secure routing mechanism, the author recommended peer-to-peer symmetric encryption to all routing information in RREQ, RREP and RERR, using a group session key negotiated by neighbour nodes. However, this design requires each node to maintain a table along with associated group members and session keys. It would become less efficient as the number of nodes in ad hoc network increases. And moreover, a compromised node could still juggle hop_count or d_seq to interrupt the normal routing procedure.

Explicitly, abnormal modification of important routing information like hop_count and d_seq in RREQ, RREP and RERR messages of AODV can not be fully prevented by the above mechanisms we found. Some attacks and misbehaviours of network nodes are still threatening AODV. For example, both the big sequence number flood and the selfish increment of hop_count. This is important motivation of our security enhancement in this paper.

Perlman [5] provides a link state routing protocol that attains Byzantine Robustness. Even though the protocol is greatly robust, it needs a very high overhead linked with public key encryption. Secure BGP [6] aims to protect the Border Gateway Protocol by using PKI (Public Key Infrastructure) and IPSec. Zhou [7] primarily discusses key management for securing ad hoc networks.

Protocol	Dynamic Source Routing (DSR) [13,14]	Ad hoc On-Demand Distance Vector (AODV)[12]	Dynamic MANET on demand (DYMO) routing protocol. (DYMO) [15]
Authors	Josh Broch, David Johnson, and David Maltz	Charles Perkins, Elizabeth Royer, and Samir Das	Ian D. Chakeres and Charles E. Perkins
Category	Reactive	Reactive	Reactive
Metrics	Shortest path, next available	Newest route, shortest path	Shortest path
Route Recovery	New route, notify source	Same as DSR, local repair	Local repair
Route repository	Route cache	Routing table	Routing table
Broadcasting	Simple	Simple	Simple
Multiple paths	Yes	No	No
Loop freedom maintenance	Source route	Sequence number	sequence numbers
Communication Overhead	High	High	High
Feature	Completely on demand	Only keeps track of next hop in route	Only keeps track of next hop in route

Table 1 Characteristic Summary of DSR, AODV, DYMO Routing Protocols[3]

	ARAN	SAODV	SRAODV	Our Solution
Source node Impersonation	Yes	Yes	Yes	Yes
Destination node Impersonation	Yes	Yes	Yes	Yes
Big Sequence Number Flood	No	No	No	Yes
Reduce the hop count	No	Yes	No	Yes
Keep the hop count unchanged	No	No	No	Yes
Selfish hop count increment	No	No	No	Yes
RERR fabrication	Yes	Yes	Yes	Yes
Not forward routing packet	No	No	No	No
Collude attack	No	No	No	No

Table2.Routing attacks protection comparison between ARAN, SAODV, SRAODV and our solution[2]

4. ATTACKS IN MANET

Classification of Attacks on MANETs Attacks in MANETs can be classified as:

- Passive attack
- Active attack

1. Passive attack

A passive attack does not actually disrupt the Operation of the operation of the network [9].

E.g. Snooping: Snooping is unauthorized access to another person's data.

- **Traffic Monitoring**
  It can be developed to identify the communication parties and functionality which could provide information to launch further attacks .It is not specific to MANET, other wireless network such as cellular, satellite and WLAN also suffer from these potential vulnerabilities.
- **Eavesdropping**
  The term eavesdrops implies overhearing without expending any expending any extra effort. In this intercepting and reading and conversation of message by unintended receiver take place. Mobile host in mobile ad-hoc network shares a wireless medium.
- **Traffic Analysis**
  Traffic analysis is a passive attack used to gain information on which nodes communicate with each other and how much data is processed.

2. Active attacks

An active attack attempts to alter or destroy the data being exchanged in the network these attacks on MANETs challenge the mobile infrastructure in which nodes can join and leave easily with dynamics requests without a static path of routing.

- **Black-Hole Attack**
  All packets are dropped by sending routing packets, the attacker could route all Packets for some destination to itself and then discard them.
- **Wormhole Attack**
  Using a pair of attacker nodes A and B linked via a private network connection every packet that A receives from ad hoc network, forwards through the wormhole to B.
- **Malign Attack**
  An attacker may blackmail a good node, causing other good nodes to add that node to their blacklists.
- **Partition Attack**
  An attacker may try to partition the network by injecting forged Routing packets to prevent one set of nodes from reaching another.
- **Spoofing Attack**
  In spoofing attack, the attacker assumes the identity of another node in the network; hence it receives the messages that are meant for that node. Usually, this type of attack is launched in order to gain access to the network so that further attacks can be launched, which could seriously cripple the network.
- **Replay Attack**
  The attacker collects data as well as routing packets and replays them at a later moment in time. This can result in a falsely detected network topology or help to impersonate a different Node identity. It can be used to gain access to data which was demanded by replayed packet.

5. CONCLUSION

Mobile Ad Hoc Network is a multi-hop wireless network of mobile nodes, structuring a temporary network with no help from several recognized infrastructure or centralized administration. Because of the lack of some committed routers, each node needs to donate towards the configuration and protection of the routing framework. As there are no centrally administered secure routers, attackers can attack the network with ease. To overcome this better routing protocol must be used. AODV is the widely used routing protocol for MANET. But this protocol fails to deliver security benefits. For providing security to MANET, SAODV is used as routing protocol for MANET. This involves the usage of digital signature, hash chains, etc., in this paper, a survey is performed on the existing routing protocols for MANET. Mainly their security support is analyzed which helps for developing better security enabled routing protocol.

REFERENCES

[1] SURVEYING SECURITY ANALYSIS TECHNIQUES IN MANET ROUTING PROTOCOLS TODD R. ANDEL, AIR FORCE INSTITUTE OF TECHNOLOGY ALEC YASINSAC, FLORIDA STATE UNIVERSITY

[2] SECURITY ENHANCEMENT OVER AD-HOC AODV ROUTING PROTOCOL Zongwei Zhou Department of Computer Science and Technology, Tsinghua University, Beijing, China , zhou-zw02@mails.tsinghua.edu.cn

[3] Performance study of Broadcast based Mobile Adhoc Routing Protocols AODV, DSR and DYMO Parma Nand1, Dr. S.C. Sharma2 1,2 Wireless Computing Research Lab, IIT Roorkee, INDIA , astya2005@gmail.com,{astyadpt, scs60fpt}@iitr.ernet.ac.in

[4] A Survey of Secure Mobile Ad Hoc Routing Protocols Loay Abusalah, Ashfaq Khokhar, and Mohsen Guizan,IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 10, NO. 4, FOURTH QUARTER 2008.

[5] Perlman, R., "Fault-tolerant broadcast of routing information", In Computer Networks, Pp. 395–405, 1983.

[6] Kent, S., Lynn, C., Mikkelson, J. and Seo, K., "Secure Border Gateway Protocol (S-BGP)", Real World Performance and Deployment Issues, 2000.

[7] Zhou, L. and Haas, Z.J., "Securing Ad Hoc Networks", IEEE Network Magazine, Pp. 24–30, 1999.

[8] C.Perkin, Elizabeth M. Royer, "Ad hoc on demand Distance Vector Routing", RFC 3561, July 2003, http.//www.ietf.org/rfc/rfc3561.txt.
[9] Surveying Security Analysis Techniques in MANET Routing Protocols, Gandhi Nirbhay Quarter, Volume 9, No. 4, 2007.
[10] Perkins C, Bhagwat P, "Highly Dynamic Destination-Sequenced Distance-Vector Routing(DSDV) Routing",SIGCOMM'94 Computer Communication Rewiev, vol 24, no. 4,p 234-244, October 1994.
[11] J.J. Garcia-Luna-Aceves, M. Spohn, "Source-Tree Adaptive Routing in Wireless Networks", Proceedings of the 7th Annual IEEE international conference on Network Protocols, Toronto, Canada. October 31- November 3, 1999. http://www.ieee-icnp.org/1999/ papers/1999-29.pdf.
[12] Charles Perkins, Elizabeth Royer, and Samir Das. "Ad hoc on demand distance vector (AODV) routing". IETF RFC No. 3561, July 2003.
[13] Josh Broch, David Johnson, and David Maltz. "The dynamic source routing protocol for mobile adhoc networks for IPv4 IETF RFC 4728, Feb 2007.
[14] D. Johnson and D. Maltz. "Dynamic source routing in ad hoc wireless networks". In T. Imielinski and H. Korth, editors, Mobile computing, chapter 5. Kluwer Academic, 1996.
[15] Ian D. Chakeres and Charles E. Perkins. Dynamic MANET on demand (DYMO) routing protocol. Internet Draft Version 06, IETF, October 2006.