The Study and Comparison between AODV, OLSR and DSR Routing Protocols and Attacks in Mobile Ad-Hoc Network

Nirmaljit Kaur
M.Tech Scholar
Department of Computer Science Engineering
Chandigarh Engineering College, Landran

Parveen Sharma
Assistance Professor
Department of Computer Science Engineering
Chandigarh Engineering College, Landran

ABSTRACT

Wireless network consist of wireless node lacking any direction. Due to current of mobility of nodes, the network is easily personated by numerous attacks. In 1980’s Movable ad hoc network s have been extensively research ` for many years. Ad hoc network is a compilation of nodes that is associated throughout a wireless medium forming speedily changing topologies. Mobile ad hoc networks are an infrastructure-less, dynamic network consisting of a collection of wireless mobile nodes that converse with each other with no the use of any centralized authority. Due to its original characteristics, such as wireless standard, self-motivated topology, dispersed collaboration, MANETs is susceptible to different kinds of safety attacks like worm whole, black hole, hastening attack etc. The communications less & active nature of these system demands new set of networking strategy to be implement in order to offer capable end to end announcement.. The study various routing protocols used in networking, performance comparison of DSR, OLSR and AODV is done. Various performance parameters measured are Throughput, End to End Delay and Packet Delivery Fraction for CBR traffic over UDP connection.

Keywords

Wireless Network, Mobile ad hoc network, black hole attack, wormhole attack and features

1. INTRODUCTION

A Mobile Ad hoc Network is a group of independent mobile nodes that can communicate to each further via radio waves. The mobile knobs that are in broadcasting range of each other can directly communicate, whereas others requirements the aid of midway knobs to route their packages. Each of the node has a wireless interface to communicate with every further. These networks are completely spread, & can work at any place without the assist of any rigid infrastructure as right to use points or base stations [1]. A mobile ad-hoc network (MANET) is a self-configuring system of movable routers (& connected hosts) linked by wireless relatives - the combination of which form an arbitrary topology. The routers are free to shift aimlessly & systematize themselves at random; thus, the system wireless topology may modify rapidly and unpredictably. Such a network may control in an impartial style, or may be connected to the larger Internet. Minimal configuration & rapid operation make ad hoc networks apposite for urgent situation situations like accepted or human induced adversity, military difference, emergency medical situations etc.

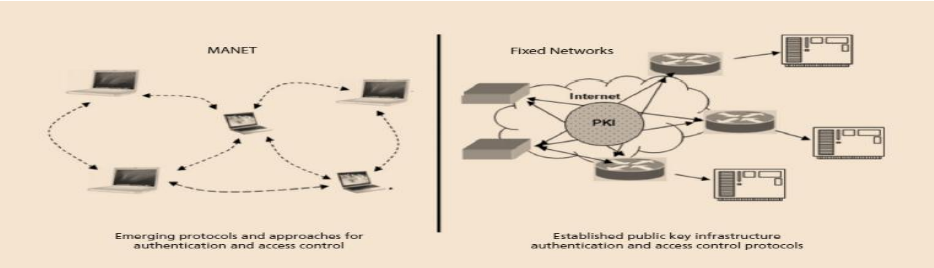
MANET
Fixed Networks
Internet
PKI
Emerging protocols and approaches for authentication and access control
Established public key infrastructure authentication and access control protocols

Fig no 1 Mobile ad-hoc network

1.1 Advantages of Manet

Some of the advantages of the Mobile ad-hoc network take in follow:

1. MANET can be succeeded where there is less telecommunication road and rail network.
2. Lowest amount cost judgment.
3. Superior flexibility.
4. MANET gives access to information and facilities apart from to geographic position.
5. This system can be arranged at any time and Place. .
6. Powerful due to decentralized organization.
7. MANET has self-regulating activities with active system topology & multi-hop system.
8. Scalable- holds the calculation of extra knobs.
9. Personality systematize network, nodes can also act as routers.

1.2 Disadvantage of Manet

Some of the disadvantages of MANET are:

1. Lack of physical safety.
2. Inherent possessions are inadequate.
3. Joint trust unsafe to attack. Deficiency of approval services.
4. Active system topology makes it difficult to identify malicious attack.[2]

2. APPLICATION OF MANET

The importance of ad hoc system has been tinted in a lot of fields which are described below:

- *Military area:* An ad hoc networking will permit the military battleground to maintain an information network among the armed forces, automobile & head office.
- *Regional level:* Ad hoc networks can build instant link between multimedia network with notebook computers or palmtop computers to increase and share information among participants.
- *Personal area system:* A personal area system is a small range, generalized network where nodes are usually associated with a given variety.
- *Industry division:* Ad hoc network is extensively used for commercial applications. Ad hoc network can also be used in crisis location such as adversity release. The quick development of non-existing infrastructure makes the ad hoc network with no trouble to be used in urgent condition.
- *Bluetooth:* Bluetooth can afford short collection communication between the nodes such as a laptop and mobile phone.[3]

3. RELATED WORK

Disha G. Kariya et al 2012[4] An adaptive method to detecting black and gray hole attacks in ad hoc network based on a cross layer design. In system layer, a course-based technique to eavesdrop the next hop's action was proposed. This scheme does not send out additional organize package & saves the scheme possessions of the detecting node. In MAC layer, a collision rate reporting scheme is recognized to guess dynamic identify threshold so as to lower the false positive rate in high system overwork. DSR protocol is favored to test algorithm**. Mehdi Medadian et al 2009[5]** Black hole attack by using cooperation with neighbors who declare to have a direction to destination. The Simulation's results show that the proposed protocol offer better safety & also improved presentation in terms of packet delivery than the conventional AODV in the attendance of Black holes with negligible supplementary setback and Overhead. **Amol V. Zade et al 2012[6]** cluster based counter calculate for the wormhole attack that improves these drawbacks and efficiently mitigates the wormhole attack in MANET. The Wormhole attack does not need make use of any nodes in the network and can interfere with the route organization procedure. They also talk about previous works which require the role of administrator and their reliance on impractical assumptions. **Kuai Xu et al 2011[7**] network-aware clustering of end hosts in the same prefixes into different performance clusters. Based on in sequence theoretical events, we find that the clusters exhibit distinct traffic characteristics which offer better explanation of the alienated traffic compared with the aggregated traffic of the prefixes. Firstly, they display the applications of discovering activities similarity in profiling network behaviors and detecting strange behaviors through artificial traffic that join Internet backbone traffic and packet traces from real condition of worm propagations & denial of service attacks. **Subhashis Banerjee et al 2013[8]** A hierarchical cluster based Wormhole attack escaping technique to shun such situation. The thought of hierarchical clustering with a novel hierarchical 32-bit knob attend to scheme is used for stay away from the attacking path during the route discovery phase of the DSR protocol, which is measured as the below deceitful routing protocol. Pinpointing the location of the Wormhole knobs in the case of showing attack is too given by using this method.

4. ATTACK ON ROUTING

There are mostly 2 types of attack are there.

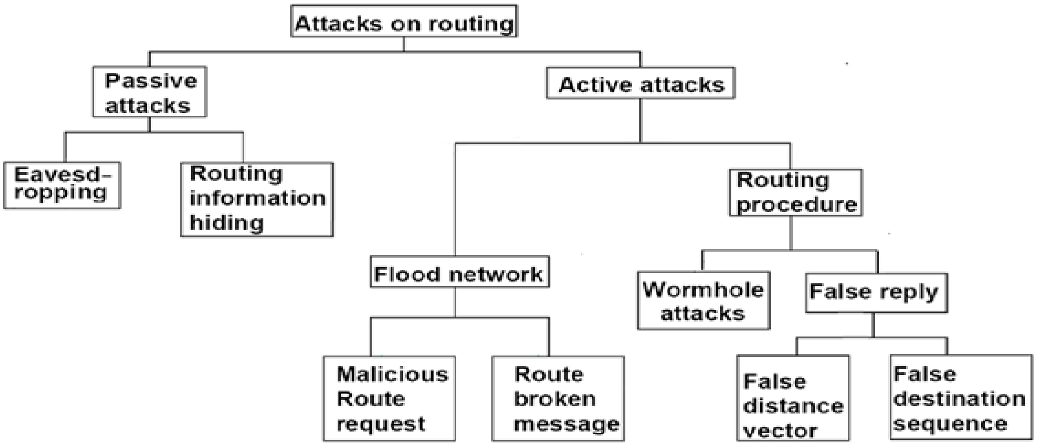

Fig no. 2 Types of Attacks

4.1 Active attack

The name of a few active attacks is Spoofing, Fabrication, Wormhole attack, Denial of services attack, Sinkhole attack, and Sybil attack.

a. Spoofing

When a malicious node miss-present his identity, so this way it can change the idea of sender & sender transform the topology.

b. Fabrication

When a malicious node generates the fake routing message. This way malicious knob produces the incorrect information about the route between devices.

c. Modification

Modification spiteful node performs a few modifications in the routing, so that sender sends the message through the elongated route. This reason time delay & announcement delay is occurred between sender and receiver.

d. Wormhole

Wormhole attack is as well call the tunnel attack. An attacker receives a packet at one point and tunnels it to one more malicious knob in the system. This method learner assumes that he found the shortest path in the network. This tunnel among 2 colluding attackers is describing the wormhole.

e. Denial of services

In this type of attack, malicious node distribution the communication to the knob & devour the bandwidth of the network. The aim of malicious node is to be busy to the system knob. This system, if a communication from the certified node will come, then receiver will not receive the message for the reason that he is busy & apprentice has to stay for the handset response.

f. Sinkhole

It is a repair attack that avoid the base station as of attain complete & accurate information. In sinkhole attack, a cooperation knob tries to draw the statistics to it starting his all adjacent node. Discerning onward, alteration or even plummeting of data can be done by the sinkhole attack.

g. Sybil

Sybil attack refers to the many copies of malicious knobs. It can be occur, if the spiteful node shares its surreptitious key with further spiteful knobs. This way the figure of malicious node is improved in the system & the prospect of the attack is as well increased. If we apply the multipath routing, then the option of decide a path in the system, those enclose the spiteful node will be increased.

4.2 Passive attack

The name of some passive attacks is overhearing something, traffic investigation, and checking.

a. Eavesdropping

It is a passive attack, which happened in the mobile ad-hoc system. The aim of nose round is to locate some secret or private in sequence that should be reserved secret through the communiqué. This secret information may be privet or communal key of dispatcher or receiver or any code word.

b. Traffic analysis

In this type of attack, an attacker attempt to sense the communiqué path among the dispatcher & receiver. This technique attacker originates the quantity of data which is travel among the route of dispatcher & receiver. There is no modification in information by the traffic examination.

c. Monitoring

Monitoring is a inactive attack in which attacker can perceive the secret information, but he cannot change the data or cannot modify the data.[9]

4.3 Flooding attack

In flooding attack, attacker wear out the system resources, such as bandwidth & to put away a node's possessions, such as computational & battery control or to dislocate the routing action to cause severe poverty in system presentation. For case in point, in AODV protocol, a malicious knob can send a large digit of RREQs in a small stage to a target node that does not stay alive in the network. since no one will respond to the RREQs, these RREQs will flood the whole system. As a result, every of the knob battery power, as well as system bandwidth will be inspired & could lead to denial-of-service.

4.4 Black hole Attack

Route finding procedure in AODV is susceptible to the black hole attack. The device, that is, any transitional knob may react to the RREQ meaning if it has a new enough way, developed to decrease routing setback, is used by the spiteful node to cooperation the system. In this attack, when a spiteful node listens to a route demand packet in the system, it responds with the claim of having the shortest and the freshest route to the purpose node yet if no such route survives. As a result, the malicious node easily misroute network traffic to it & then fall the packages temporary to it.

4.5 Rushing Attack

Nodes, which also take delivery of the similar route request Rushing attacks are mainly against the on-demand routing procedure. These kinds of attacks undermine the route discovery process. On-demand routing protocols that utilize spare repression during the route detection process are vulnerable to this attack. When compromised node receives a way demand packet as of the source knob, it floods the packet quickly throughout the network before additional package can react. [10]

5. ROUTING PROTOCOLS

Routing protocols are usually alienated into 3 main classes; Proactive, reactive & hybrid protocols. Categorization of MANET routing procedure:

5.1 Proactive procedure

Proactive, or table-driven steering protocols. In proactive routing, each node has to maintain single or more tables to accumulate routing information & a few changes in network topology need to be reflected by broadcast keep informed throughout the system in arrange to maintain a consistent network view.

Example of such schemes is the conservative routing system: Target sequenced distance vector (DSDV). They attempt to maintain consistent, up-to-date direction-finding information of the total system. It reduces the delay in statement and allows nodes to rapidly determine which knobs are nearby or available in the system.

5.2 Reactive Protocols

Reactive direction-finding is as well-known as on-demand routing protocol since they do not maintain routing information or routing movement at the system knobs if there is no announcement. If a node needs to send a package to a different knob then this procedure searches for the way in an on-demand mode & found the association in order to broadcast and receive the package. The way discovery occurs by overflow the way demand packets all through the system.

Example of reactive routing procedure is the Ad-hoc On-demand Distance Vector direction-finding (AODV) and Dynamic Source Routing (DSR).

5.3 Hybrid Protocols

They set up a hybrid model that unites reactive & practical routing protocol. The Zone Routing Protocol (ZRP) is a hybrid routing protocol that separate the system into zones. ZRP supply a hierarchical architecture where every knob has to maintain extra topological information requiring extra memory. [11**]**

There are three routing protocol is used in this paper. And the protocols are selected based on the flat routing protocol. Flat routing protocol distributes routing information to routers that are connected to each other without any organization or segmentation structure between them. The four protocols are act as loop free routing Like that, quick route access, and reduce the packet loss and improve the efficiency of route reconfiguration and less delay (see in table 1).

Table no: 1 Difference between DSR, OLSR and AODV

PARAMETER	DSR	OLSR	AODV
Routing structure	Flat	Flat	Flat
Rout acquisition	High	Low	High
Control overhead	Medium	High	Low
Loop free	Yes	Yes	Yes
Updates transmitted to	Source	Neighbor	Source

6. CONCLUSION

MANET due to their active behavior, incomplete resources (control, bandwidth etc.), and distributed operation is more vulnerable to many attacks. MANET is more vulnerable to many attacks. In this paper, we discuss MANET and its characteristics, challenges, compensation, application, safety goals, different types of security attacks in its routing protocols. Security attack can classified as active or passive attacks and also the protocols are better for PDR, End to End Delay and Throughput than Table driven (proactive) protocols. The hybrid protocol AODV performs worst and hence is the worst MANET Routing Protocol. DSR performs better than both OLSR and AODV.

7. REFERENCES

[1] Aarti, Dr SS. "Tyagi,"Study Of Manet: Characteristics, challenges, application and security attacks"." International Journal of Advanced Research in Computer Science and Software Engineering 3, no. 5 (2013): 252-257.

[2] Yadav, Meenakshi. "Survey on MANET: Routing Protocols, Advantages, Problems and Security." (2014).

[3] Helen, D., and D. Arivazhagan. "Applications, advantages and challenges of ad hoc networks." JAIR 2.8 (2014): 453-7.

[4] Kariya, Disha G., Atul B. Kathole, and Sapna R. Heda. "Detecting Black and Gray Hole Attacks in Mobile Ad Hoc Network Using an Adaptive Method."international journal of emerging technology and advanced engineering 2, no. 1 (2012).

[5] Medadian, Mehdi, Ahmad Mebadi, and Elham Shahri. "Combat with Black Hole attack in AODV routing protocol." Communications (MICC), 2009 IEEE 9th Malaysia International Conference on. IEEE, 2009.

[6] Hu, Yih-Chun, Adrian Perrig, and David B. Johnson. "Rushing attacks and defense in wireless ad hoc network routing protocols." Proceedings of the 2nd ACM workshop on Wireless security. ACM, 2003.

[7] Xu, Kuai, Feng Wang, and Lin Gu. "Network-aware behavior clustering of Internet end hosts." In INFOCOM, 2011 Proceedings IEEE, pp. 2078-2086. IEEE, 2011.

[8] Banerjee, Subhashis, and Koushik Majumder. "ANovel CLUSTER BASED WORMHOLE AVOIDANCE ALGORITHM FOR MOBILE AD-HOC NETWORKS." ICCSEA, SPPR, CSIA, WimoA–2013..

[9] Shrivastava, Satyam, and Sonali Jain. "A brief introduction of different type of security attacks found in mobile Ad-hoc network." ACM/Kluwer Wireless Networks Journal (ACM WINET) 9, no. 5 (2003).

[10] Wu, Bing, et al. "A survey of attacks and countermeasures in mobile ad hoc networks." Wireless Network Security. Springer US, 2007. 103-135.

[11] Holter, Kenneth. "Comparing AODV and OLSR." folk. uio. no/kenneho/studies/essay/essay. html (2005): 1-19.

[12] Macker, Joseph, and Scott Corson. "Mobile ad hoc networks (MANET)." (1997): 35-42.