Hybrid Protocol for Handling Security using SBPGP

Pooja Chahal
Department of computer science
Lovely Professional university
Phagwara, India

Gaurav Kumar Tak
Department of computer science
Lovely Professional University
Phagwara, India

ABSTRACT

A mobile ad hoc network is part of wireless networks which is formed by collection of two or more nodes moving in an arbitrary manner. The nodes are self organizing, adaptive, infrastructure less and has dynamic topology. Hence due to high mobility and multipath propagation network is vulnerable to attacks. There are many types of MANET like VANET (Vehicular Ad hoc Network), SPANs (Smart Phone Ad hoc Networks), iMANET (Internet based Mobile Ad hoc Network), Tactical MANET. There are various attacks that can be possible on MANET like Denial of Service attack, Black hole attack, Wormhole attack, Sybil attack etc which can disturb the communication between the nodes. So today's requirement is to provide secure and authentic communication in MANET. For small network security is not a big issue but for large or complex network security should be provided in large extent. To provide security for complex networks in the network using a technique Seniority Based Pretty Good Privacy (SBPGP) is used.

Keywords

AOMDV, Black hole attack, DOS, MANET, Network Security, SBPGP.

1. INTRODUCTION

An ad hoc network is a network that is formed by collection of two or more nodes (devices) that moves in an unpredictable manner. One node can communicate that is within its radio range or outside their radio range. The data is forwarded from one to another node with the help of intermediate nodes. An ad hoc network is infrastructure less, self organizing, adaptive. It follows an infrastructure less architecture yet has a potential of service discovery, routing and packet forwarding. These networks are autonomous and decentralized in nature. The nodes present in network can anytime join or leave the network. All nodes should be able to find the presence of other nodes so that further communication and sharing of data can take place. Examples of ad hoc network are palmtop, laptop, Internet mobile phones etc [1]. Ad hoc wireless devices can take any form so the computation, storage communication capabilities are also different. As there is diversity in the wireless devices so the battery capacity also varies tremendously from one device to another device. There are no routers or access points in wireless network so nodes themselves act as router. These nodes can make different topologies based on the connectivity with each other in the network. As stated earlier these nodes are self-organizing it means that they can be deployed anywhere without any planning or infrastructure. So there is urgent requirement of security.

1.1. TYPES OF ADHOC NETWORK

There are two types of Ad hoc network

a) SANET (Static Ad hoc Network)

In Static ad hoc network the geographic conditions and stations are fixed. As soon as nodes are deployed they are fixed. There is no mobility and that's why this type of networks is termed as SANET.

b) MANET (Mobile Ad hoc Network)

MANET is a part of wireless networks. No wires and fixed routers are used in this type of network. It is not everlasting network; it is the short term network. Nodes has the capability to self organize themselves and it follows infrastructure less architecture. Network is formed by number of nodes moving in an inconsistent manner. They do not form any topology. And every nodes further acts as routers which transfers packet from one node to another node [2].

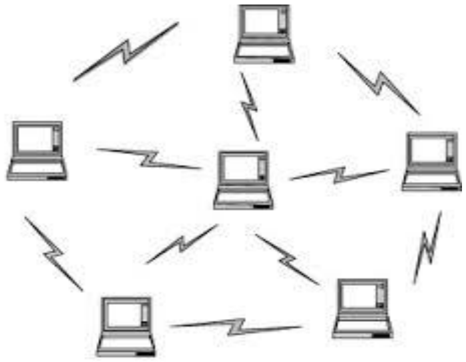

Figure 1: MANET

2. ROUTING PROTOCOLS

As MANET is infrastructure less, node frequently moves from one place to another and so secure routing is required and it is done with the help of routing protocols. The main aim of routing protocols is to dynamically exchange information of networks paths from source to destination and select the best path to reach the destination.

Classification of routing protocols:

1) Table Driven or Reactive

2) On Demand or Proactive

3) Hybrid

2.1 Table driven routing protocol

The main aim of table driven routing protocol is to maintain up-to-date routing information from each and every node present in the network. Every node has to maintain one or two routing table to store all the information of nodes and whenever nodes moves from one place to another place, this route update should be in the node routing table to maintain a consistent network [3].

2.2 On Demand Routing Protocol

In this route is discovered only when it is required .When node wants to start the communication then it will check its route cache if it exists then the communication will take place and if route is not there then it demands form route discovery process and as soon as it will finds the route it starts its process. There are mainly two processes in on demand routing protocol [3].

Route discovery When node wants to communicate with another node and if the route is not present in its cache it will initiates route discovery process. The source node then contains the destination address and the addresses of intermediate nodes.

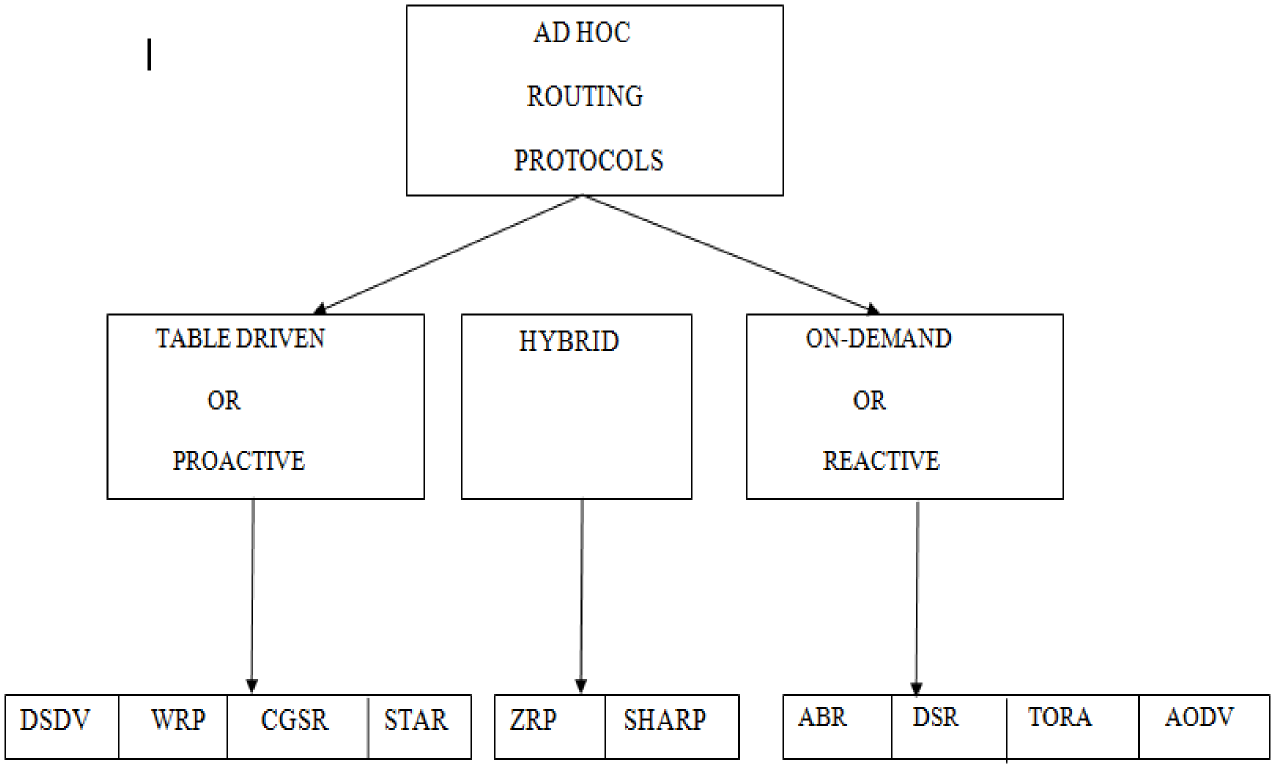

Figure 2: Routing protocols

Route maintenance As the topology is dynamic each node is free to move so there are link breakage which can hamper the network so it is very important to maintain the route and it is done by route maintenance process.

2.3 Hybrid routing protocol

It is a combination of proactive routing protocol and reactive routing protocol. It deals with the shortcomings of both table driven and on demand routing protocols. It uses route maintenance process of table driven protocol and route discovery process of on- demand routing protocol. Hybrid protocol is used in large networks [3].

3. SECURITY

Security is one of the major issues in wireless network. These networks are vulnerable to attacks. Securing ad hoc network form attacks is very challenging. Once the unauthorized person gets access to the network then he can misuse it. Attacks can be categorizes into two type active attack and passive attack. In passive attack the intruder only keep tracks of data that is being transfer between the hosts. There is no modification or fabrication of data. Eavesdropping and traffic analysis are examples of passive attacks. In active attack intruder modify the data. Examples of active attacks are modification, replay, and denial of services. There are some more attacks like black hole, wormhole, grey hole, Sybil, sleep deprivation attacks that has great impact on ad hoc networks. As soon as a node becomes malicious node it hampers the communication. So there is need of secure routing and secure routing protocol that can provide security against the malicious behavior of nodes [4].

There are many attacks or security problems in MANET:

1. Dos attacks: It is an attempt to make the network unavailable to the users [4].

2. Resource consumption: An attacker wants to consume all the resource like power or battery. Example of resource consumption attack is sleep deprivation attack.

3. Host impersonation: A node impersonate legitimate node and misuse the network. It is also known as spoofing attack. 4. In this attack attacker wants to get the secret information like public key, passwords etc that should be disclosed in the communication.

4. Information disclosure: In this attack an attacker obtains all the information and discloses this information to the third party.

5. Interference: Whenever any interference occurs in the network it reduces network performance such as delay, throughput, data loses etc.

6. Black hole attack: In this type of attack all the packets are dropped by the malicious node and fake packets are further send [4].

7. Wormhole attack: In this attack all the data or information is collected at one point, tunnels it and displayed it to the other point [4].

4. LITERATURE REVIEW

Moukhtar A. Ali, Ayman EL-SAYED classified multicast routing protocols according to different parameters like multicast topology, topology maintenance, topology initialization, core or coreless approach. The author also focuses on the concept of how to apply multicast routing in MANET's and the considerations that each protocol should achieve robustness, efficiency, scalability, security and quality of service (QOS).

Maqsood Razi and Jawaid Quamar had proposed a security model for small networks using Seniority based trust model and PGP type authentication service. Author also explained some of the related algorithm such as mechanism of certification authentication and certificate revocation mechanism. Then the performance is estimated and author concluded that the particular model is easy, reliable, efficient and easy to deploy.

Jashanvir Kaur and Er. Sukhwinder Singh Sran described about the security with the help of Public Key Infrastructure (PKI), Pretty Good Privacy (PGP), and Seniority Based Pretty Good Privacy (SBPGP). There are many models that provide security to small networks using PGP so the author focused on providing security to large networks. Her paper describes the concept of PKI, technologies related to PKI and comparison of PKI based model. And the results show that SBPGP gives better result as compared to other PKI techniques.

Jaya Jacob, V.Seethalakshmi had estimated the performance of routing protocols in MANET like DSDV, AODV, DSR, TORA and AOMDV. He also introduces new protocol that is a modification in AOMDV and it is known as modified AOMDV (Energy_AOMDV). This protocol improves the battery power of individual node. Author concluded that AOMDV is best protocol among AODV, DSR, TORA and DSDV but when he compared AOMDV and Energy_AMODV, the result shows that Energy_AOMDV is better that AOMDV.

Dr. S.S. Dhenakaran and A.Parvathavarthini had discussed about types of routing protocol. Routing protocols are mainly categorized into three types proactive, reactive and hybrid. The protocols that are discussed in this paper are DSDV, WRP, CGSR, DSR, AODV, ABR, TORA, ZRP and SHARP.

Boundpadith Kannhavong, Hidayamaehisa Nakyama et.al had discussed all the attacks possible on the MANET. Attacks are black hole, colluding misrelay attack, link spoofing attack, wormhole attack, replay attack, message withholding attack, flooding attack. Author also discussed about the advantage, disadvantages and countermeasures of each attack.

Nidh Mittal , Janish had focused on providing security with Public Key Infrastructure (PKI) and its various types in MANET. The Seniority based pretty good privacy (SBPGP) technique is applied on two routing protocols AODV and DSDV protocol. Result shows that end to end delay and throughput of AODV is better that DSDV but delivery packet fraction of AODV is low.

5. PROPOSED WORK

As MANET is infrastructure less, self organizing, adaptive in nature. These networks are vulnerable to many types of attacks and one the attack is DOS attack. The main aim of this attack is that the attack intentionally sends hundreds of packet simultaneously so that the server gets down or the network become unavailable to the users who wants to access it. Then these attacks malfunction in the network which degrades the network performance. DOS attack is one of them. There are many techniques to prevent or control this attack. But each technique may slow down the process of data transfer. So there is need for some improvement in routing protocol to transfer the data at high speed. So Seniority based pretty good privacy (SB P.G.P) is used to provide some authentication and security in the network.

The protocols on which work has to be carried out are DSR and AOMDV.

5.1 Dynamic Source Routing (DSR):

DSR is reactive routing protocol and it uses source routing process. This protocol uses Link state routing algorithm in which source initiates the route discovery process only on demand basis. In this no HELLO packets are exchanged between nodes. Sender is only aware of the path between the source to destination and intermediate nodes.

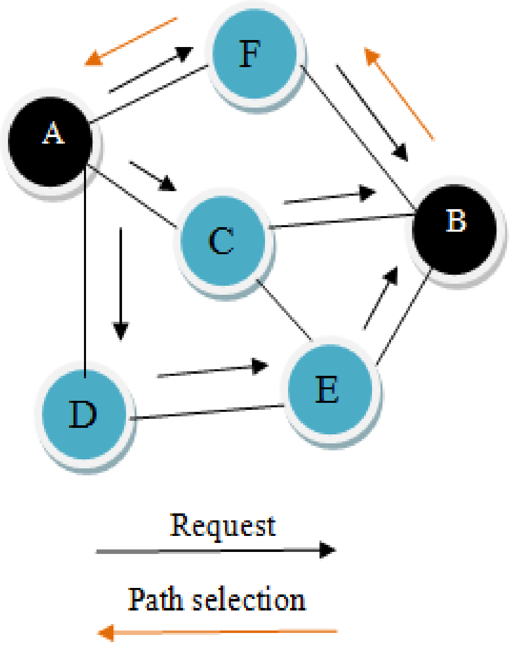

Figure 3: Dynamic Source Routing

5.2 Ad hoc on Demand Multipath Distance Vector Routing

AOMDV protocol is the advanced version of AODV protocol. It uses hop-by hop routing and distance vector mechanism. Both AODV and AOMDV protocol work on reactive (on demand) routing protocol. That is, whenever there is demand to find the routes then only it starts its route discovery process. In AOMDV, when RREQ request is sent from sender to receiver it generates multiple reverse paths on both receiver node and intermediate node. Then multiple RREP requests travel through these reverse path to form forward paths [13].

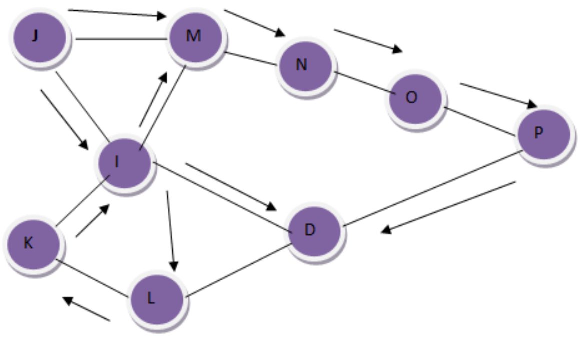

Figure 4: Routing path with multipath computation in AOMDV

5.3 Hybrid Algorithm (Hybrid approach to merge these two protocols)

```
Algorithm 1 send data
If route exist && energy> threshold
Then send (packet DATA)
Else
    For each NODE
        If co-ordinates of node are in between sender and destination
        Then send (packet RREQ)
        Endif
    endfor
    i=0
    repeat
        if NTT is elapsed then NTT=NTT*2 endif
        i=i+1
    until i>=3 and no RREP is received
    if  RREP is received then
        update the routing table
        send DATA to destination
    else cannot reach the destination
    endif
endif
endif
```

```
Algorithm 2 receive_RREQ
If source.RREQ_ID< node.RREQ_ID then drop the packet RREQ
Else
    update the reverse route to the source if necessary
    if node know a path to destination then send the packet RREP
    else
        save the Previous_IP into RREQ_LIST
        if source.RREQ_ID>node.RREQ_ID then update RREQ
        update node.RREQ_ID
        Foreach NODE
            If node’s co-ordinate is in between sender and destination
            Then send packet RREQ
            Endif
        endfor
    endif
endif
```

```
Algorithm 3 receive_RREP
Delete from the RREQ_LIST the node whose address is equal to RREP_PREVIOUS_IP
Send the packet RREP only to the nodes whose addresses are stored in RREQ_LIST.
```

5.4 Security Model

5.4.1 SB-Trust Model

In this work for issuing PGP type certificate we have applied SB model. Suppose a MANET is established in an area where many people are communicating with each other and the wireless channel over which they are communicating is not secure. Let us consider there are N nodes and they are randomly moving from one place to another and any mobile node if free to join or leave the network at any time. In this scenario the mobile nodes that joined the network at the beginning are said to be senior nodes and the nodes that joined the network later on that are said to junior nodes [5].

For the construction of model some assumptions are there:

- Every node has a nonzero ID and it should be unique
- Every node that is present in the network has a mechanism to recognize the senior nodes in that particular network
- Communication in the is consistently good and authentic with senior nodes rather than junior nodes
- Every senior node has some local detection method by which they can easily detect the malicious nodes or misbehaving nodes among its surrounding nodes.

In this model two or more senior nodes collectively form a Certifying Authority (CA). Whenever a new node comes in the network these senior nodes will check all the information about that new node and if they are satisfied with the information then only they collectively sign on the certificate of new node [8].

SN = ceiling (N × M %) + 1

SCA = ceiling (SN × K%) + 1

JN = N – SN

Where

SN is senior nodes

JN is junior nodes

N is total number of node in the network

SCA is set of nodes required for CA functionality

M is variable %

K is variable % (depends on M)

6. CONCLUSION AND FUTURE SCOPE

The given study focuses on analysis of various routing protocols and as it has been known that attacks can decrease the performance of communication protocol. Many protocols have the capability to handle it at some extent but when the network is complex and have multipath then performance degradation occurs. So in this work two protocols one is dynamic source Routing (DSR) and another one Ad hoc on demand distance vector routing Protocol (AOMDV) are combined to make a hybrid protocol by using the hybrid algorithm that is explained above and then the security mechanism i.e. Seniority based pretty good privacy will be applied on it. Protocol performance would be tested in higher mobility situations. This work will optimize performance metrics like end-to-end delay, packet delivery fraction, and throughput, energy efficiency and round trip time. Also this work will show good result in terms of energy and time and also provides security to the network by means of certification number. In future this technique can be applied to various multicast routing protocols like Multicast Routing Protocol Based on Zone Routing (MZRP) and Associativity-Based Ad Hoc Multicast Routing (ABAM).

7. ACKNOWLEDGEMENT

I am very grateful to Lovely professional University and faculties for their constant support and encouragement.

8. REFERENCES

[1] Toh, C.K. 2001. Ad hoc mobile wireless networks: protocols and systems. Pearson Education.

[2] Aarti., Tyagi, S.S. 2013. Study Of Manet: Characteristics, Challenges, Application AndSecurity Attacks. International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013 ISSN: 2277 128X, pp. 252-257.

[3] Ali, M., Sarwar. Y. 2011. Security Issues regarding MANET (Mobile Ad Hoc Networks): Challenges and Solutions, Thesis no: MCS-2011-11.

[4] Chahal, P., Tak, GK., Tomar, AS. 2015. Comparative analysis on various attacks on MANET, International Journal of Computer Applications (0975 – 8887) Volume 111 – No 12, February 2015.

[5] Kaur, J., Sran, SS. 2012. SBPGP Security based Model in Large Scale Manets, International Journal of Wireless Networks and Communications. ISSN 0975-6507 Volume 4, Number 1 (2012), pp. 1-10

[6] Kannhavong, B., Nakayama, H., Nemoto, Y., Kato, N. 2007. A Survey Of Routing Attacks In Mobile Ad Hoc Networks. Ieee Wireless Communications.

[7] Ali, MA., EL-SAYED, A., Z.Morsi, I. 2007.A survey of multicast routing protocols for ad-hoc wireless networks. Minufiya Journal of Electronic Engineering Research (MJEER), Volume 17, No.2.

[8] Maqsood, R., Quamar.2008. A Hybrid Cryptography Model for Managing Security in Dynamic Topology of MANET, Biometrics and security Technologies, ISBAST 2008, Internation Symposium on IEEE, 2008 , pp. 1-7.

[9] Jacob, J., Seethalakshmi, V. 2012. Performance analysis and enhancement of routing protocol in MANET, International Journal of Modern Engineering Research (IJMER), ISSN: 2249-6645, pp -323-328.

[10] Dhenakaran, S.S., Parvathavarthi, A. 2013. An Overview of Routing Protocols in Mobile Ad-Hoc Network. International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 2, February 2013, ISSN: 2277 128X.

[11] Kannhavong, B., Nakayama, H., Nemoto, Y., Kato, N. 2007. A Survey Of Routing Attacks In Mobile Ad Hoc Networks. Ieee Wireless Communications.

[12] Mittal, N., Janish. 2013. Performance Evaluation of AODV and DSDV under Seniority Based Pretty Good Privacy Model (SBPGP). International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013 943 ISSN 2229-5518.

[13] Marina, MK., Das, SR. 2006. Ad hoc on-demand multipath routing protocol, Wireless communication and mobile computing.khiavi, MV., Jamali, S. 2013. Performance comparison of AODV and AOMDV Routing Protocols in Mobile Ad hoc network, International Research Journal of Applied and Basic Sciences, ISSN 2251-838X / Vol, 4 (11): 3277-3285.