International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 01 | Jan-2016 www.irjet.net p-ISSN: 2395-0072

A SURVEY ON SECURED ROUTING IN AD HOC NETWORKS FOR VARIOUS ATTACKS

R.Mythily[1], L.Raja [2]

[1]*PG student, ECE, K.S.R college of Engineering, Tamilnadu, India.*

[2]*Associate professor, ECE, K.S.R college of Engineering, Tamilnadu, India*

Abstract - ***Wireless ad hoc network doesn't depend on any infrastructure; they are vulnerable to several security threats. Secure and efficient communication is one of the most important aspects in ad hoc wireless networks, so its need to develop a protocol strategy which utilizes the bandwidth efficiently, takes less power and produce better performance. Mobile Ad Hoc Network (MANET) is one of the most important and unique application. Malicious packet dropping is a serious attack against this network. In this attack, an adversary node tries to drop all or partial received packets instead of forwarding them to the next hop through the path Security is an essential service for wired and wireless communications. The success of MANETs strongly depends on people's confidence in its security. Variety of security mechanisms has been invented to counter malicious attacks. There are several efficient routing protocols have been proposed for MANET. Here I reviewed various routing protocol and security issues due to various attacks in ad hoc networks and considering security requirements as well security mechanism***

KEY WORDS: *Wireless ad hoc network, routing protocol, MANET, malicious packet dropping, various attacks security issues, security requirement and mechanisms*

I.INTRODUCTION

1.1 Mobile Ad Hoc Network (MANET)

Infrastructure-less networks are autonomous system of mobile nodes and can be connected dynamically in an arbitrary manner. All nodes of these networks behave as routers and take part in route discovery and maintenance of routers to other nodes in the network. These kinds of networks are very flexible, thus, they do require any infrastructure or central administration. Therefore, mobile ad-hoc networks are suitable for temporary communication links. A mobile ad hoc network (**MANET**) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. Ad hoc is Latin and means "for this purpose". As per Pranjali. D. Nikam, Vanita Raut MANET is vulnerable to malicious attacks due to its open medium and wide distribution of nodes [2] . To adjust to the growing trend of MANET in industrial applications, it is vital to address its potential security issues. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology.

1.2 TYPES OF ATTACKS

The main challenges in assuring MANET networks are due to the fact that a mobile link is susceptible to attacks, and node mobility renders the network to having a highly dynamic topology. The attacks against routing protocol can be categorized into external and internal attacks and also classified into passive and active attack.

i) External vs. Internal attacks: External attacks, in which the attacker aims to cause congestion, propagate fake routing information or disturb nodes from providing services. Internal attacks, in which the adversary wants to gain the normal access to the network and participate the network activities, either by some malicious impersonation to get the access to the network as a new node, or by directly compromising a current node and using it as a basis to conduct its malicious behaviours.

ii) Passive Attacks: As per [5] Adnan Nadeem a passive attack does not disrupt the normal operation of the network; the attacker snoops the data exchanged in the network without altering it. Here the requirement of confidentiality gets violated. Detection of passive attack is very difficult since the operation of the network itself doesn't get affected. One of the solutions to the problem is

to use powerful encryption mechanism to encrypt the data being transmitted, thereby making it impossible for the attacker to get useful information from the data overhead.

iii) Active Attacks As per Adnan Nadeem an active attack attempts to alter or destroy the data being exchanged in the network there by disrupting the normal functioning of the network [5]. Active attacks can be internal or external. External attacks are carried out by nodes that do not belong to the network. Internal attacks are from compromised nodes that are part of the network. Since the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks.

1.3 SECURITY ISSUES

In [1] as per Sumimol L, Janisha some of the security issues are followed.

1. Insecure channel: Channel is open radio broadcasting one so messages can be eavesdropped and fake messages can be injected or replayed into the network, without the need to access the network components.

2. Insecurity of the nodes: Nodes may not be physically protected, and more vulnerable to attacks. If an attacker accesses a node, it can change its behaviour, or corrupt the hardware

3. Absence of infrastructure: Ad hoc networks have no fixed infrastructure. So security mechanisms used for normal wired scenario will not be applied for this Ad Hoc.

4. Dynamically changing topology: - The topology of a wireless networks is quickly changing.

5. Quality of Service: Due to the dynamic nature of the medium the Quality of service will not be ensured completely.

II.ROUTING PROTOCOL CLASSIFICATION

In ad hoc networks, nodes act as a router. Routing is the process of selecting path in a network along which to send network traffic. A specific set of communication rules by which computers can communicate with each other is a protocol. Classification of routing protocol is shown in figure 1. Since Routing protocol specifies how routers can communicate with each other. It use metrics to find which path is best for the packet to travel in the network Metrics is the stand of measurement like Bandwidth, Delay, Reliability and current load on the path. To establish a valid, efficient and secure route between a pair of nodes is the goal of the routing protocol then only messages delivered in a timely manner. Routing protocols are generally classified into three types.

i) Proactive Routing Protocols
ii) Reactive/Ad hoc Based Routing protocols
iii) Hybrid Protocols

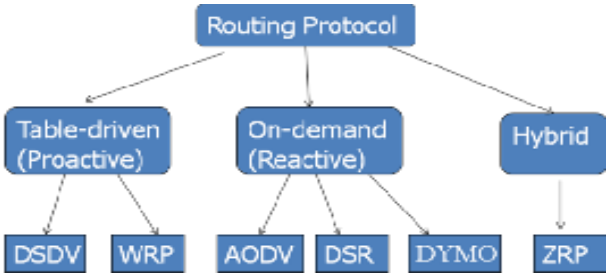

Figure: 1 Classification of routing protocol in mobile ad-hoc network

i) PROACTIVE ROUTING PROTOCOL

It is also known as Table Based. Maintain routes between every host pair all the time, Shortest-path protocols, frequently update routing table; high routing overhead. Table-driven routing protocols try to keep the last updated and stable routing information from each node to the rest of the nodes in the network. In this type of routing protocol, each node should maintain at least one table to store the routing information. In case of any change in the network topology, the nodes will propagate the route updates throughout the network in order to maintain a stable network view.

Destination Sequence Distance Vector (DSDV)

DSDV has one routing table, each entry in the table contains: destination address, number of hops toward destination, next hop address. Routing table contains all the destinations that one node can communicate. When a source A communicates with a destination B, it looks up routing table for the entry which contains destination address as B. Next hop address C was taken from that entry. A then sends its packets to C and asks C to forward to B. C and other intermediate nodes will work in a similar way until the packets reach B. DSDV marks each entry by sequence number to distinguish between old & new route for preventing loop. DSDV use two types of packet to transfer routing information: full dump and incremental packet. An example of DSDV routing protocol is shown in figure 2 with the node 2 routing table. DSDV has advantages of simple routing table format, simple routing operation and guarantee loop-freedom. The disadvantages are (i) a large overhead caused by periodical update (ii) waste resource for finding all possible routes between each pair, but only one route is used.

Routing Table for Node 2

Destination	Next Hop	Metric	Dest. Seq. No.
1	1	1	123
2	0	0	516
3	3	1	212
4	4	1	168
5	4	2	372
8	1	INF	432

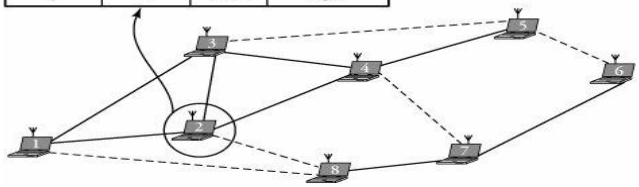

Figure: 2 DSDV Routing Protocol

Wireless Routing Protocol (WRP)

The Wireless Routing Protocol (WRP) is a proactive, destination-based protocol. WRP belong to the class of path finding algorithms. The typical feature for these algorithms is that they utilize information about distance and second-to-last hop (predecessor) along the path to each destination. Path-finding algorithms eliminate the counting-to-infinity problem of distributed Bellman-Ford-algorithms by using that predecessor information, which can be used to infer an implicit path to a destination and thus detect routing loops. In WRP there is a quite complicated table structure. Each node maintains four different tables as in many other table-driven protocols only two tables are needed. These four tables are: 1) distance table, 2) routing table, 3) link cost table and 4) message retransmission list (MRL) table.

ii) REACTIVE ROUTING PROTOCOL.

It is also known as On-demand provides Source initiates route discovery. Here, the routing protocols create routes only when requested by the source node. A route discovery process is initiated by the source node. This process is considered done either after: Finding a route to the destination and after examined all the possible route permutations. Once the route is established, it will be maintained by some form of route maintenance procedure until either the destination becomes inaccessible or the route is no longer desired.

Ad Hoc On Demand Distance Vector (AODV)

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 diagram of AODV protocol is shown in figure 3. 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.

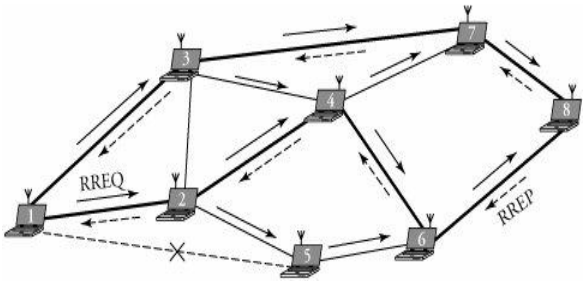

Figure: 3 AODV Routing Protocol

Dynamic Source Routing (DSR)

The DSR is an on-demand routing protocol for wireless network, it relies on source routing instead of routing table at each intermediate nodes. As per S.Ranjithkumar1 [8] To accomplish source routing, the routed packets contain the address of each device the packet will traverse, which result in high overhead or large addresses, like IPv6. The DSR routing protocol is shown in figure 4. 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.

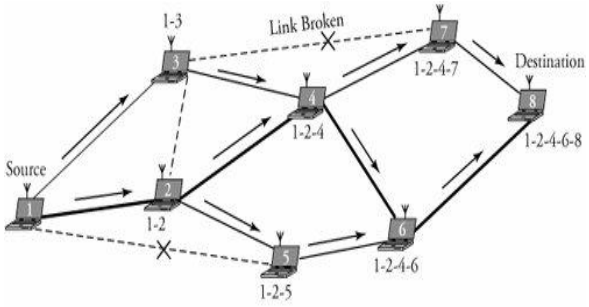

Figure: 4 DSR Routing Protocol

Dynamic Mobile Ad hoc Network On-demand (DYMO)

DYMO routing protocol has been proposed by Perkins & Chakeres as advancement to the existing AODV protocol. It is also defined to as successor of AODV and keeps on updating till date. DYMO operates similar to its predecessor i.e. AODV and does not add any extra

modifications to the existing functionality but operation is moreover quite simpler. In [4] as per Anuj K DYMO is a purely reactive protocol in which routes are computed on demand i.e. as and when required. Unlike AODV, DYMO does not support unnecessary HELLO messages and operation is purely based on sequence numbers assigned to all the packets. It employs sequence numbers to ensure loop freedom. It enables on demand, multi-hop unicast routing among the nodes in a mobile ad hoc network. The basic operations are route discovery and maintenance. In [6] as per Sukant The DYMO Route discovery process is shown in figure 5 Route discovery is performed at source node to a destination for which it does not have a valid path. And route maintenance is performed to avoid the existing obliterated routes from the routing table and also to reduce the packet dropping in case of any route break or node failure. DYMO implements three messages during the routing operation namely Route Request (RREQ), Route Reply (RREP) and Route Error (RERR).

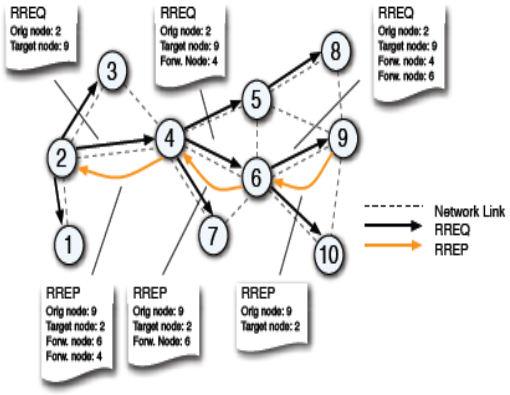

Figure: 5 DYMO Routing Protocol

iii) HYBRID ROUTING PROTOCOLS

Combination of proactive and reactive is Hybrid protocol. To overcome the drawbacks in proactive and reactive protocol it is used. It reduces the control overhead of proactive routing protocol and delay which occur due to initial route discovery in reactive routing protocol

Zone Routing Protocol (ZRP)

Zone routing protocol was the first hybrid routing protocol with both a proactive and a reactive component. ZRP was proposed to reduce the control overhead that of proactive routing protocols and decrease the latency as caused in routing discover in reactive routing protocols Routes are easily available for nodes inside the zone, but a route discovery process has to be employed by ZRP for nodes outside the zone. The routing zones of neighbouring nodes overlap with each other's zone. Each routing zone has a radius ρ that is expressed in hops. The zone includes the nodes whose distance from the source node is at most ρ hops. Routing zone of radius 2 hops for node A is shown as in figure 6 All the nodes except node L are included in the routing zone, because It lies outside the routing zone node A. The routing zone is not expressed as physical distance, rather is defined in hops. In ZRP nodes in a routing zone can be categorized as:

1) Peripheral Nodes - nodes with minimum distance to central node that is exactly equal to the zone radius p
2) Interior Nodes - nodes with minimum distance less than the zone radius ρ

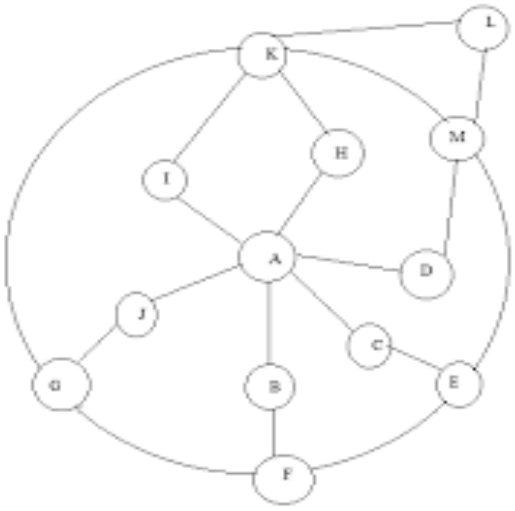

Figure: 6 Routing Zone of Node A with Radius ρ=2 hop

III.SECURITY REQUIREMENTS AND MECHANISM

3.1 SECURITY REQUIREMENTS

There are five major security goals that need to be addressed in order to maintain a reliable and secure ad-hoc network environment. As per Ming Yu However, the characteristics of MANET pose both challenges and opportunities in achieving security goals, such as confidentiality, authentication, integrity, availability, access control, and non-repudiation [7].

1. Confidentiality is to keep the information sent unreadable to unauthorized users or nodes.
2. Authentication is to be able to identify a node or a user, and to be able to prevent impersonation.
3. Integrity is to be able to keep the message sent from being illegally altered or destroyed in the transmission.
4. Non-repudiation is related to a fact that if an entity sends a message, the entity cannot deny that the message was sent by it.
5. Availability is to keep the network service or resources available to legitimate users.

3.2 SECURITY MECHANISMS

As per Ashish Kumar Jain MANETs in general lacks security mechanism [3]. A variety of security mechanisms have been invented to counter malicious attacks. The conventional approaches such as authentication, access control, encryption, and digital signature provide a first line of defence. As a second line of defence, intrusion detection systems and cooperation enforcement mechanisms implemented in MANET can also help to defend against attacks or enforce cooperation, reducing selfish node behaviour.

1. Preventive mechanism: The conventional authentication and encryption schemes are based on cryptography, which includes asymmetric and symmetric cryptography. Cryptographic primitives such as hash functions (message digests) can be used to enhance data integrity in transmission as well. Threshold cryptography can be used to hide data by dividing it into a number of shares. Digital signatures can be used to achieve data integrity and authentication services as well.

2. Reactive mechanism: An intrusion detection system is a second line of defence. They are widely used to detect misuse and anomalies. A misuse detection system attempts to define improper behaviour based on the patterns of well-known attacks, but it lacks the ability to detect any attacks that were not considered during the creation of the patterns; Anomaly detection attempts to define normal or expected behaviour statistically. It collects data from legitimate user behaviour over a period of time, and then statistical tests are applied to determine anomalous behaviour with a high level of confidence.

IV CONCLUSION

Ad hoc network is a group of wireless mobile computers for temporary communication The aim of this paper is to provide an overview of various routing protocol and security issues due to various attacks in ad hoc networks and also considering security requirements as well security mechanism Adding Security mechanism to the routing protocols can reduces the level of problems like dynamic topology, selfish nodes, multihop packet relay and attacks

V REFERENCES

[1] Sumimol L, Janisha A "Security in Wireless Adhoc Networks based on Trust and Encryption" International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 6, June 2015.

[2] Pranjali. D. Nikam, Vanita Raut "Enhancement to EAACK for improved MANET security" International Journal of Advanced Research in Computer Science and Management Studies,Volume 3, Issue 5, May 2015.

[3] Ashish Kumar Jain, Vrinda Tokekar " Mitigating the Effects of Black hole Attacks on AODV Routing Protocol in Mobile AdHoc Networks" International Conference on Pervasive Computing (ICPC), 2015.

[4] Anuj K. Gupta1, Harsh Sadawarti2 and Anil K. "Implementation of Dymo Routing Protocol" Verma3 International Journal of Information Technology, Modeling and Computing (IJITMC) Vol.1, No.2, May 2013.

[5] Adnan Nadeem, Michal P.Howarth " A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks" IEEE communication surveys & tutorials, 2013.

[6] Sukant Kishoto Bisoyi, Sarita Sahu "Performance analysis of Dynamic MANET On demand (DYMO) Routing protocol" Special Issue of IJCCT Vol.1 Issue 2, 3, 4; 2010 for International Conference [ACCTA-2010], August 2010.

[7] Ming Yu, Mengchu Zhou, Wei Su " A Secure Routing Protocol Against Byzantine Attacks for MANETs in Adversarial Environments" IEEE Transaction on vehicular technology, vol.58, no. 1, January 2009.

[8] S.Ranjithkumar1, N. Thillaiarasu2, "A Survey of Secure Routing Protocols of Mobile AdHoc Network" SSRG International Journal of Computer Science and Engineering (SSRG-IJCSE) – volume 2 issue 2 February 2015