IJRSET SEPTEMBER 2017 Volume 4, Issue 9 Pages: 1-7

ISSN 2394-739X

International Journal for Research in Science Engineering and Technology

A SURVEY AND ANALYSIS OF MANET'S ENHANCING SECURITY TECHNIQUES AND ROUTING PROTOCOLS

[1] A. Mahendran , [2] Dr. C. Kavitha
[1] Ph.D Research Scholar ,[2] Assistant Professor
[1,2] Dept of Computer Science, Thiruvalluvar Govt Arts College
[1,2] Periyar University, Rasipuram, Salem-11

ABSTRACT: Ad hoc Networks (MANETS) are transient networks of mobile nodes, connected through wireless links, without any fixed infrastructure or central management. Mobile Adhoc Network is a dynamic network formed by a collection of wireless nodes. As it is a dynamic network all the nodes involved in the network must play the role of a router at some point of time. Due to the self-configuring nature of these networks, the topology is highly dynamic. In this paper, we survey the common security threats, attacks and summarize the solutions suggested in the survey to mitigate these security vulnerabilities and enhancing security techniques and routing protocols for MANET.

Keywords: [Manet, Routing Protocols, Techniques, Security Attacks]

1. INTRODUCTION

Mobile Ad hoc Network (MANET) is a collection of infrastructure less mobile devices connected by wireless medium. The mobility of nodes results in change in position of nodes. The lack of access point results in more network activity where topology discovery and message forwarding must be routed by the node themselves. In modern years, MANETs have been developing rapidly and are being used in many applications, ranging from civilian, military and commercial applications. Since setting up of such networks can be done without the help of any infrastructure or interaction of a human. Some examples are: search-and-rescue missions, data collection, and virtual classrooms and conferences where PDA, lap-tops or other mobile devices share wireless medium and communicate to each other. Routing is one of the major problems of networking to deliver packets from one node to the other in the network. A Manet's uses peer-to-peer multihop routing to provide network connectivity. MANETs can be characterized as having dynamic, multihop, and rapid changing topology. There are lots of issues in designing an ad-hoc network. Because of rapid changing topology, nodes changes its position on every second this is one of the major challenge is link failure. Route selection can also be considered as one of the major issue in routing protocol. Selecting non-optimal routes may increase delays, routing loads, decrease throughput and increase loss rate since the selected route will break quickly or nodes get congested. Most of the traditional ad hoc routing protocols use hop count as a metric for selecting paths from source to the destination. MANET is low in bandwidth and in dynamic shape, our popular technologies like cell phones, PDA, digital handheld devices, laptops and even an MP3 player may be the participant in MANET. We use term "mobility" for MANET, which means that one may move freely. No base station or access point participates in MANET, and it can easily be applicable that is why it is used in different military operations because MANET can be designed at run time. In case of natural disasters when all existing infrastructure is destroyed, we use MANET technologies for different rescue operations in this circumstances. Bluetooth is modern wireless technology. The goal in MANET is to design Bluetooth that may be used to connect with others. Every protocol has its own advantages and limitations. We can list few weaknesses of MANET as –Limited bandwidth, low battery power, computational power, security etc.

2. LITERATURE SURVEY

R. Khan, A. M. N. Azad. and S. A. Vishwakarma evaluates the performance of various ad-hoc routing protocols such as DSDV, AODV, DSR, TORA and AOMDV on the basis of energy efficiency and they also proposed a routing algorithm that not only modifies AOMDV but also give better performance as compared to all the above protocols. Proposed Energy-AOMDV protocol performs better in case of packet delivery ratio (PDR), throughput, jitter and average end to end delay. The packet drop in case of Energy-AOMDV is less than AOMDV. **U. R. Bhatt, P. Jain and R. Upadhyay** presents an EERP-protocol based on AODV. This protocol reduces the transmission power of a node which is a part of an active route if next hop node is closer. A method is proposed the distance between two consecutive nodes is calculated based on RSS (received signal strength) from next hop during route reply process. If RSS is high, it implies nodes are closer; as a result lesser transmission power will be required to selection done on the basis of residual energy, traffic density and the stability of the node until the time T. RREP packets are broadcasts along the paths. Power loss level is calculated by subtracting received energy from transmitting energy along the particular path. Data packets are sending through the path having low power loss level. **S. Kurundkar and A. Maidamwar** presents an improved AODV protocol. Stability factor is used to calculate the remaining energy of nodes. The stability of a node is defined as the ratio of its remaining energy to the initial energy. **Sanjay Ramaswamy et al.** proposed a solution for cooperative black hole attacks by slightly modified AODV Routing Protocol by introducing Data Routing Information (DRI) Table and Cross Checking. This algorithm is based on a trust relationship between the nodes. **Vishnu K et al.** discussed a Backbone Network which is based on selecting some trustworthy and powerful nodes in terms of battery power and range. These nodes which are referred to as Back Bone Nodes (BBN) will form a Back Bone network and have special functions unlike normal nodes. This algorithm detects black hole as well as gray hole attack in AODV. **Deng et. al.** has proposed an algorithm to prevent black hole attacks in ad hoc networks. According to the algorithm, any node on receiving a RREP packet, crosschecks with the next hop on the route to the destination from an alternate path. If the next hop either does not have a link to the node that sent the RREP or does not have a route to the destination then the node that sent the RREP is considered as malicious. This solution cannot prevent cooperative black hole attacks. Apart of that there are many techniques which are used for the security of AODV.

transmit data and reduces battery consumption. **R. Rajeshkanna and A. Saradha** proposed that protocol path

3. PROPERTIES OF AD-HOC ROUTING PROTOCOLS

Routing is the process of forwarding packets from source to destination using most efficient route. Efficiency of the path/route is measured in various metric like number of hops, traffic, security etc. The main goal of routing protocols is to minimize delay, maximize network throughput, maximize network lifetime and maximize energy efficiency. All MANET routing protocols could be broadly classified into three major categories: Pro-active Routing Protocols, Reactive Routing Protocols, and Hybrid Routing Protocols. 1) Proactive routing protocol: In proactive routing scheme every node continuously maintains complete routing information of the network. This information is stored in tables. Each node maintains a routing table which contains the list of destinations and routes. 2) Reactive routing protocol: The reactive routing protocols are based on some sort of query-reply dialog. In this the nodes do not need periodic transmission of topological information of the network. When there is a need for a route to a destination, route request messages are flooded periodically with new networks status information. Every node in this routing protocol maintains information of only active paths to the destination nodes. 3) Hybrid Routing Protocols: Often reactive or proactive feature of a particular routing protocol might not be enough. These protocols combined the features of both reactive and proactive routing protocols.

A. Ad-hoc On demand Distance Vector (AODV): Route is initiated by the node which needs to communicate with a destination only on a demand. The source initiates path finding through RREQ to its one hop neighbors. The packet is forwarded by an intermediate node its one hop neighbors if it is not a destination. On reception of this RREQ at destination, A RREP is generated and sent back to the source. Nodes store only the active route information which results in reduced control overhead.

B. Dynamic source Routing (DSR): In DSR path finding is almost similar as in AODV. No periodic exchange of control packets. During packet forwarding in intermediate nodes, not like AODV, they store their ID and update their cache with the active routing information. Route discovery and recovery are done only when it is required. Routing overhead is scaled to the actual size.

C. Cluster-based routing protocol (CBRP): Nodes are organized in a hierarchical manner and grouped into clusters. Each cluster is represented using a cluster-head. Data transmission is done through the cluster heads between the clusters which reduces the control overhead.

D. Fisheye State Routing (FSR): Each node stores the link state for every destination in the network. This link state update of a destination is periodically broadcasted to its neighbors. Update messages contain information only about closer nodes and not farther.

E. Zone Routing Protocol (ZRP): This hybrid protocol acts as both reactive and proactive routing protocols. Within a zone it acts as a proactive routing protocol using Intra Zone routing protocol (IARP). Between zones it acts as a reactive protocol using Inter Zone Routing Protocol (IERP). Path can be constructed to destination node within the local region using the proactively cached routing information. If the destination is away from the local region then the route discovery is done reactively through the border nodes. The border nodes pass the request by adding their ID to the RREQ to the next zone if the destination is not within the local zone.

F. Link Aided Routing (LAR): Network identifies two zone namely requested zone and expected zone. Instead spreading the RREQ packets to the entire network, the packets are sent to the zones where the destination is expected to be. Using an algorithm with the GPS location the requested zone is obtained. The source node estimates the expected zone of the destination based on the previous location. The RREQ is flooded only to the requested zone inclusive of the expected zone.

G. On-Demand Anonymous Routing in Ad Hoc networks (ODAR): Initial routing process of ODAR follows DSR algorithm. The protocol uses a data structure called bloom filter which stores a set of element. Each element is tested if it is a member of the set or not. Elements involved in the set or permanent. Once if the source hashes the route information it cascades it to the bloom filter. An intermediate node will forward the packet if and only if its ID is in the bloom filter, otherwise it will simply drop the packet.

H. Link State Routing (LSR): Route is found using Dijkstra's shortest path method based on current conditions. Each node has topology view of the entire network and is updated regularly through link state packet (LSP). This is circulated among the neighbour nodes till all are updated.

I. Optimal Link State Routing (OLSR): OLSR is a proactive routing protocol. The routing information is updated periodically through the nodes one hop neighbor selected namely multipoint relay (MPR). The traffic and control overhead is reduced as the packets are sent through the MPRs.

J. Destination-Sequenced Distance Vector (DSDV): In DSDV sequence numbers are assigned by each source while in the network maintain routing information to all known destinations and route updates are done periodically. route request packets are sent to neighbours, which avoid looping and help to select a latest route. Global view of network topology is not available. All the nodes

K. Privacy-Preserving Location-Based On-Demand Routing in MANETs(PRISM): Routing is done based on AODV and do not propagate topology information. PRISM mainly concentrates on the security aspect against the insider and outsider attacks. Hash of RREQ, RREP is used as a route identifier and group signatures are used for authentication.

L. Secure Position Aided Ad hoc Routing (SPAAR): Along with the destination ID, distance from the source and exact coordinates are included. Specialty of SPAAR is that the routing information is encrypted with a group encryption key. The receiving node decrypts the information and the successful nodes informing the sender are the one hop neighbors. Similarly the remaining route estimation is done at the intermediate nodes by adding their IDs to the RREQ. The route cache is maintained for the reverse path. RREP generated at the destination is also in an encrypted form of details like sequence number, velocity, destination's coordinates and timestamp.

M. Anonymous On-Demand Routing in Mobile Ad Hoc Networks (MASK): The node identities are masked with the help of a group pseudonym. In order to find the path, first the node which needs to communicate authenticates the neighboring node by sending a challenge with the pseudonym selected in random. Then the master key is calculated by the challenged node and gives authentication to the sender. Based on the master key both of them generate link ID and session keys.

N. Anonymous Routing Protocol for mobile ad hoc networks (ARM): The RREQ is generated in such a way that the nodes except destination cannot be aware of the destination. With the help of the pseudonym the intermediate nodes can conclude that they are not the destination node. For each communication a secret key and current pseudonym are shared between the source and destination. The destination sends the RREP in an encrypted for with its broadcast ID.

O. Efficient Anonymous Dynamic Source Routing for Mobile Ad-Hoc Networks (AnonDSR): The communication process involves three protocols in different levels. At first level a shared key and a nonce is generated between the source and the destination. Using this trapdoor is created in second level. Each intermediate node has a shared session key. Finally after the route discovery the communication is done using this session key.

P. Anonymous Location-Aided Routing in Suspicious MANETs (ALARM): Nodes are grouped on location basis and are lead by a group manager. Each node register itself with the group manager gets a group signature. The protocol sends Location Announcement Messages (LAM) from time to time to the nodes in the group. The LAM message has details like nodes current position, time stamp and a session key. Only valid members with the signature can decrypt the packets and read. Concatenation of nodes temporary ID and the group signature forms the pseudonym.

Q. A Geocasting Protocol for Mobile Ad Hoc Networks Based on GRID (GeoGRID): Geographic area is divided as a number of grids. Each grid has a grid leader. Only the leader can propagate the packets tp the members in the grid. GeoGRID is available I two versions namely flooding-based and ticket-based. GeoGRID is appreciated well in crowded MANET.

R. Security Aware Routing protocol (SAR): SAR aims at security based on the trust values and trust relationships associated with adhoc nodes and this value is used to take routing decisions. Security is provided through symmetric encryption method. Routing is done only through trusted nodes to which trust values are already assigned. Nodes which satisfy the required level of security only can participate in routing.

S. Signal Stability Based Adaptive Routing (SSA): In SSA the routes are analyzed and categorized as strong and weak nodes based on their signal stability. This protocol works on an on demand basis. During path finding the node selection is done through the strong nodes. Channeling **T. Temporally-Ordered Routing Algorithm (TORA):** TORA follows a hierarchical topology of nodes. Route construction is done on a directed acyclic graph (DAG) form. Information always flows from the higher level to the lower level as a fluid. The node which requires communicating with the destination node will find path through the upper node in upper level.

4. TECHNIQUES TO MITIGATE VARIOUS SECURITY ATTACKS IN MANET'S

Different techniques that are proposed to enhance and fortify the ad hoc routing protocols against various security loopholes and vulnerabilities in the ad hoc networks.

1. Solution Using Trust Values

These solutions mitigate various security vulnerabilities and enhance the existing ad hoc routing protocols. Trust among nodes is calculated using a combination of direct and indirect trust. When the trust value of a node declines so much that it falls below a threshold, it is then added to a blacklist. A message trust based solution to the multipath routing scenario. Based on the behavior of the nodes the assigned trust value is either incremented or decremented. Trust values may be positive, negative or zero, indicating known, malicious, or unknown behavior. In this subsection, various trust value based solutions have been discussed. These solutions mitigate various security vulnerabilities and enhance the existing ad hoc routing protocols.

2. Wormhole Detection Method

The main aim of the wormhole attack is to replay the packet on the other side of the network. This attack is executed by two nodes colluding to form a wormhole. The attacker on one side make the nodes believe that distance to the destination is just one hop, when it is greater than one hop. This causes the attacker to attract all the traffic from one side of the network and relay it through the wormhole; the attacker on the other side replays the same packet. By doing this the attacker can drop the packets or obtain any service illegally.

3. Intrusion Detection Systems (IDS)

A feature list is created to distinguish between the normal and anomalous behavior. The Intrusion detection system is a method for detecting the attacks by analyzing and continuously monitoring network functions. Intrusion detection arises as a crucial defensive mechanism in mobile ad hoc networks. Intrusion detection systems would be deployed in each mobile node to monitor local traffic and to detect occurrence of local intrusions. These nodes can forward the intrusion information to neighbors when needed.

4. Black-hole detection and prevention

The purpose of this attack is to increase the congestion in network. In this attack the malicious node does not forward any packets forwarded to it, instead drops them all. Due to this attack the packets forwarded by the nodes do not reach their intended destination and the congestion in the network escalates due to retransmissions.

5. Sink-hole Detection and Prevention Method

First Fast Second Reliable (FFSR) that ensures the transfer of data packages in the shortest and the most reliable mode. The routing metric in this method is based on the cognition of each node and all the nodes in cognitive ad hoc network collect information about the whole network periodically.

6. Multi-Factor Authentication Techniques

This idea can very easily be extended to provide better security in ad hoc networks protocol. In this technique has been used to prevent impersonation in ad hoc networks.

CONCLUSION

Mobile Ad hoc network is a collection of mobile nodes and having no central administration. In this paper have surveyed the various routing protocols with their advantage and disadvantages. Since, nodes in the network have dynamic topology. As we know that, nodes are battery powered and depend on energy for transmitting or receiving packets in the network. We explained each of the security techniques and the properties of routing protocol on the ad hoc networks. In future work will choose any one techniques and routing protocols which is most secure and suitable to do better accuracy for network security process and then apply some enhancement within that to proof much better than the old performance.

REFERENCES

[1] R. Khan, A. M. N. Azad. and S. A. Vishwakarma, “Enhancement of MANET Routing Protocol”, 978-1-4799-3064-7/14/$31.00, 2014 IEEE.

[2] U. R. Bhatt, P. Jain and R. Upadhyay, “Enhanced AODV – An Energy Efficient Routing Protocol for MANET”, 2013Nirma University International Conference on Engineering (NUICONE), IEEE.

[3] R. Rajeshkanna and A. Saradha, “Energy Efficient Enhanced AODV Routing Protocol for mobile Ad hoc Network”, IJCTA, vol. 4, (2013).

[4] S. Kurundkar and A. Maidamwar, “Improved-AODV Routing Protocol for Mobile Ad hoc Networks”, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE), vol. 2, iss. 7, (2013).

[5] Sanjay Ramaswamy; Huirong Fu; Manohar Sreekantaradhya; John Dixon; and Kendall Nygard (2003). Prevention of cooperative black hole attack in wireless Ad hoc networks. In Proceedings of 2003 International Conference on Wireless Networks, (ICWN'03), Las Vegas, Nevada, USA, pp. 570-575.

[6] Vishnu K and Amos J Paul, “Detection and Removal of Cooperative Black/Gray hole Attack in Mobile Adhoc Networks”, International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 22, 2010.

[7] Hongmei Deng, Wei Li, and Dharma P. Agrawal, ”Routing Security in Wireless Ad Hoc Network”, IEEE Communications Magzine, vol. 40, pp. 70-75, 2002.

[8] Karlsson, Jonny; Dooley, Laurence S. and Pulkkis, Goran, “Routing Security in Mobile Ad-hoc Networks”. Informing Science and Information Technology Education 2012 Conference (InSITE’12), 22-27 June 2012, Montreal, Canada (Forthcoming), 2012.

[9] Ashwani Garg, Vikas Beniwal, “A Review on Security Issues of Routing Protocols in Mobile Ad-Hoc Networks”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 9, pp.145-148, September-2012.

[10] Preeti Bathla, 2Bhawna Gupta, “Security Enhancements in AODV Routing Protocol”, IJCST Vol. 2, Issue 2, June 2011.

[11] Adnan Nadeem and Michael Howarth, “Protection of MANETs from a range of attacks using an intrusion detection & prevention system”, Springer.

[12] K. SIVAKUMAR, Dr. G. SELVARAJ, “Overview of Various Attacks in Manet and Countermeasures for Attacks”, Vol 2, Issue 1, ISSN 2278-733X, January 2013.