IJCSE International Journal of Computer Sciences and Engineering Open Access

Survey Paper Vol.-6, Issue-10, Oct 2018 E-ISSN: 2347-2693

A Survey of Routing Protocols and Security Issues in MANET

K. Sumathi[1*], D. Vimal Kumar[2]

[1,2]Dept. of Computer Science, Nehru Arts and Science College, Coimbatore, India

[*]*Corresponding Author: sumathiisri5@gmail.com, Tel.: 9952536422, 9788618550*

Available online at: www.ijcseonline.org

Accepted: 20/Oct/2018, Published: 31/Oct/2018

***Abstract*—**Mobile Ad-hoc network (MANET) is a type of ad hoc network that can change locations and configure itself on the fly and wireless communications. The mobile nodes communicate with each node without any centralized manner. The MANETs does not have any pre-defined network topology. The MANET node wants to send the data between two nodes to establish wireless connection to exchange the data. After data sending is finished the connection is ended. The mobile network topology is regularly changing the location due to nodes moving, resource limitation and bandwidth limitation of mobile node. There are many types of routing protocol available in MANET. In this paper, we discuss about different type of existing MANET routing protocols and its security problems. The MANET routing protocols offered for secure packets sending and face some common attack in ad hoc networks. The routing protocol are subjected to situation against the most frequently identified attack sink hole, grey hole, spoofing, black hole attack and wormhole attack etc. A survey of various issues in MANET regarding security is done considering all major aspects.

***Keywords*—** Mobile Ad-hoc Network, Security Issues, Routing Protocols, Attacks.

I. INTRODUCTION

The mobile ad hoc network (MANET) is usually defined as a network that has numerous allowed or independent nodes, often collected of mobile node or other mobile node, that can arrange themselves in many ways and function without severe top-down network topology. A Mobile Ad-hoc Network (MANET) is a group of mobile nodes connected to the wireless links able to dynamically form an autonomous multi-hop radio network without the use of any pre-existing organization. Intermediate nodes in a MANET can act as forward the packet of other nodes. The self-forming nature and their ability to cope with fast changes of the topology, ad-hoc networks are attractive to a variety of applications.

The routing protocols for MANETs try to maintain the communication between a pair of nodes (source-destination) in spite of the position and velocity changes of the nodes. To achieve that, when those nodes are not directly connected, the communication is carried out by forwarding the packets, by using the intermediate nodes.

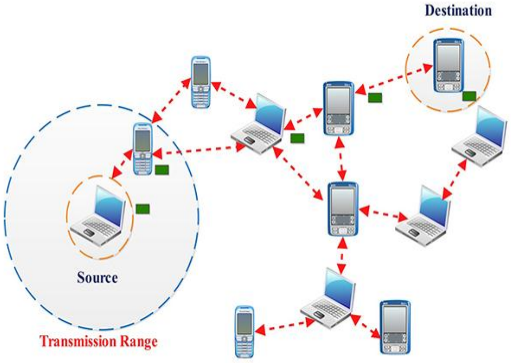

Figure 1. Overview of MANET

The Advanced ad-hoc network motivates numerous applications and studies in recent research authors. The ad-hoc network node is self-organized, these will need advanced security over wireless network. Due to limited communication and resources constrain it becomes problematic to provide security for ad-hoc network. The group wireless node communication for is common for ad-hoc network which need data to be transmitted in a secure and trusted way. The wireless network security has to attain security goals (1) Confidentially, to prevent the data from unauthorized interpretation transmitted dated, (2) The message authentication used to stop tempering with transmitted packet. The source node message authentication is the validation that message has not been altered and the sender of a message is as requested to be, this can be done by cryptographic digital signature algorithms and message authentication techniques, the primary involve asymmetric cryptography and often needs high resource consumption and high computation time at the sender and receiver side. The medium access control (MAC) indirectly ensures message and source truthfulness. The one to one communication in shared security system used for MAC generation.

In existing research solve many challenges in MANET network are complex to provide group communication in ad hoc network. The wireless nodes in ad-hoc network have limited computing, bandwidth, and energy resources which make the high overhead. Another problem unstable wireless links due to intrusion cause many packets loss error and require a good security solution that includes retransmission and reply done the packet loss. The last problem same common key will make a problem of imitating source by any receiver by attacker, so solution has to be made for using multiple authentications over the network without network overhead.

Rest of the paper is organized as follows, Section II contain overview of MANET and type of MANET routing protocols, Section III contain some security issues in MANET, Section IV contain types of attacks and comparison of recent attack detection algorithm and remarks explain, Section V concludes.

II. MANET PROTOCOLS

In MANET routing protocol is a significant purpose for wireless network. The mobile Ad Hoc Networks (MANETs) are considered as there are no special routers in MANETs.

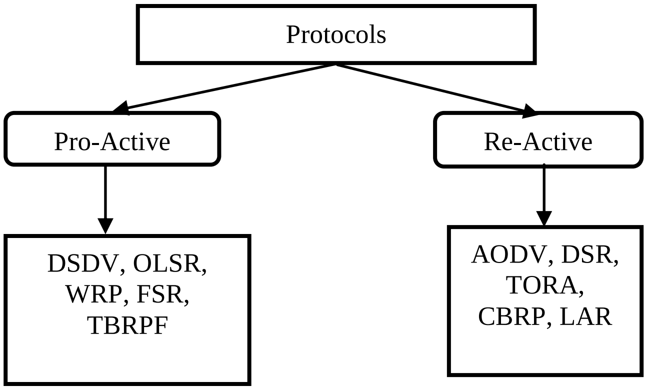

Figure 2. Type of Routing Protocols

A. Proactive Routing Protocols

Proactive routing protocol (table driven routing) to maintain recent routing information in the routing table. The information concerning the connectivity of every node to all other nodes that contribute in the network. The proactive routing, these protocols allow every node to have a clear and reliable view of the network topology by broadcasting periodic information updates. Therefore, all nodes are able to make instant decisions regarding the forwarding of a specific packet.

- Destination Sequenced Distance Vector (DSDV)

Destination Sequenced Distance Vector (DSDV) is a one node by one node vector routing protocol requiring each node to continuous route request broadcast to neighbor nodes to updates routing information. The DSDV routing protocol based on alterations to the Bellman-Ford routing mechanism this algorithm routing the packet to the shortest path between the source to destination. In DSDV every node in the wireless network keeps a routing table that has admissions for each of the destinations in the network. Each routing table entry has a sequence number associated with it that helps in recognizing stale entries. This protocol to avoid the packet looping. Every node periodically sends updates information throughout the network node with a monotonically increasing even sequence number to promote its location. Suppose new route broadcasts cover the address of the destination, the number of hops to reach the destination node, the sequence number of the information received about the destination, as well as a new sequence number unique to the broadcast. The route considered with the most recent sequence number is always used to forward the packet to next node. When the neighbors of the transmitting node receive this update, they recognize that they are one hop away from the source node and include this information in their distance vectors. Each node stores the “next routing hop information” for every reachable destination in their routing table.

- Optimized Link State Routing Protocol (OLSR)

The Optimized Link State Routing (OLSR) is another type of table-driven protocol, OLSR routing protocol future routing link history for MANETs. The optimization of pure link state protocols in that it reduces the size of route request and route response packet as fine as the number of control packets transmission required to reduce the network overhead. The OLSR reduces the control traffic overhead by using Multipoint Relays (MPR), which is the important idea behind OLSR protocol. The MPR is a node's one-hop neighbor which has been selected to forward packets. Instead of existing pure flooding of the network, packets are just forwarded by a node's MPRs. This restricts the network overhead, thus being more effective than pure link state routing protocols. The OLSR is well suitable to large area network and dense mobile networks. The MPRs, the larger and denser a network, the more improved link state routing is attained. MPRs also help to shortest path packet routing to a destination. The MPRs state the link information for their MPR selectors. The wireless topology information is preserved by periodically conversation link state information. If additional reactivity to topological changes is required, the time interval for swapping of link state information can be reduced.

B. Reactive Routing (On-demand) Protocol

On-demand routing protocols (Reactive routing), which is best most used protocol in ad hoc networks, this protocol cannot keep up-to-date information about the network topology, as is done by the proactive protocol, but they make routes on demand-based routing packet. The reactive routing protocols, the Ad hoc On Demand Distance Vector Routing (AODV) and the Dynamic Source Routing (DSR) are the greatest established and general ones. This kind of protocols finds a route on demand by flooding the entire network with route request packets to get routing information.

- Ad hoc On Demand Distance Vector Routing

Another on-demand routing protocol like AODV to builds routes source node send the route request packet throughout the network to form the routing table. AODV is consequently considered an on-demand based algorithm and does not make any additional traffic for communication along links. The AODV routes are preserved as long as they are required by the source's node. This protocol also forms trees to connect multicast group node. AODV makes use of sequence numbers to ensure route freshness routing information. The self-starting and loop-free routing also scaling to numerous wireless nodes. In AODV, topology is silent until connections are recognized. Wireless nodes that essential connections broadcast a request for connection. The AODV nodes forward the data and record the node that demanded a connection. Thus, they create a sequence of temporary routes back to the requesting node. A node that receives such information and holds a route to a desired node sends a backward message through temporary routes to the requesting node. The node that started the request uses the route covering the least number of hops through other nodes. The accesses that are not used in routing tables are recycled after approximately time. If a link fails, the routing error is passed back to the transmitting node and the process is frequent.

- Dynamic Source Routing

The Dynamic Source Routing protocol (DSR) is an effective routing protocol planned specifically for use in multi-hop packet routing wireless ad hoc networks of mobile nodes. This protocol allows the network to be entirely self-configuring and self-maintain network, without any existing network infrastructure or old routing information. The protocol is self-possessed of the two main devices of "Route Discovery" and "Route Maintenance", this two-type packet together to allow nodes to learn and keep routes to random destinations in the ad hoc network. All features of the protocol function entirely on-demand, allowing the routing packet overhead of DSR to scale routinely to only that needed to respond to variations in the routes currently in use.

- Cluster-Based Routing Protocol (CBRP)

Cluster based routing protocol is a in mobile ad hoc networks to form the network in cluster head. The protocol used to divide the network into a number of overlapping two-hop-diameter clusters in a spread manner. The cluster head is elected based on residual energy for each cluster to maintain cluster membership information. Inter cluster node routes are discovered dynamically using the cluster membership information reserved at each cluster head. The clustering nodes into groups, the protocol efficiently minimizes the routing overhead and life time of the network during route discovery and speeds up this process as well.

III. SECURITY ISSUES IN MANET

The MANET's have many security problems, there are some important metrics in MANET approaches call them "Security parameters". Actuality unaware of these parameters may cause a many security problem useless in MANET. The security algorithm with respect to MANET network are susceptible compromises, particularly at the end of low-end devices due to weak protection. The attacker enters into the network and poses weakest link and incur a domino effect of security in the wireless network. The wireless channel is concerned bandwidth is one of forced and use to part among multiple different network nodes.

The MANET in recent research working and solved many problems. The application of MANET's variety from wireless home and office networking to sensor networks and similarly constrained strategic network environments. In security features play a significant role in nearly all of these application scenarios given the weaknesses inherent in wireless ad hoc networking from the very detail that radio communication takes place to routing, man-in-the-middle and intricate data injection attacks.

1) Privacy: - privacy is a term which is generally used to provide information for persons who have been official to access that available information. Keep the information secret from all of the unauthorized node. since of this may be attacker nodes can interrupt or terminate the information. So, privacy is important in wireless network. To maintain the confidential information from the unauthorized wireless node.

2) Accessibility: - accessibility is that security standards in which an object should maintain its capability into its security standards for provide the all of the designed facilities. Some malicious information or nodes can make the service unobtainable.

3) Integrity: -Integrity is a term in which information that will be transmitted, is never interrupt or destroy. It can be done in two ways.

   i. Suppose the information is demolished & fake by an attacker with some malicious data, is called the malicious changing.

   ii. Suppose the information is misplaced or its some content are changed due to packet failure, which might be transmission faults in approval fault, then it called the accidental changing.

4) Verification: - The verification security standards firstly protect that a node into the communication are not an illegal node. Occasionally into act the authentication period, the malicious node act as cooperative node and thus attempts to access the private information or can insert the fake messages to disturb the network process.

5) Authorization: - Any unauthorized individual cannot act like as the authorized individual to access any private information. This is used to deliver various different access privileges to various types of nodes.

6) Non-repudiation: - Non-repudiation is a packet sending source and destination of an information cannot deny that they have sent or received a packet. This is valuable at that time when try to examination about the malicious nodes which are continuously attempts to disturb the network processes between various authorized nodes.

7) Attacks using construction: - construction is a process in which untruthful routing messages are produced and there is very problematic to detect such kinds of messages.

IV. ATTACKS ON MANET

The mobile ad hoc network can be focus to various types of attacks. In mobile ad hoc network, attacks can be classified into passive attacks and active attacks. Here explain details of both attacks is as follow:

Passive Attacks: Passive attacks are the attack that does not disrupt correct process of network. The attackers spy data swapped in network without changing it. The confidentiality can be desecrated if an attacker is also able to take data gathered through interfering. The detection of these attack is problematic operation of network itself does not get affected.

- Traffic Monitoring
- Eavesdropping
- Traffic Analysis
- Syn flooding
- Active Attacks

Active attacks: The active attack is achieved by the malicious nodes that tolerate some energy cost in demand to achieve the attacks. The active attack can change the data information or creation of false information. Active attacks may be internal or external. External attacks are approved out by nodes that do not belong to the network. Internal attacks are after compromised nodes that are share of the network. The attacker is previously part of the network, internal attacks are more severe and hard to detect than external attacks. Active attacks, whether accepted out by an external advisory or an internal compromised node contains actions such as takeoff, modification, construction and replication.

- Black hole Attack.
- Wormhole Attack.
- Byzantine attack.
- Rushing attack.
- Sinkhole.
- Spoofing Attack.
- Jamming Attack.
- Sybil attack.
- Sinkhole attack.
- Denial of service attack.
- Gray-hole attack.
- Selfish Nodes.

V. RECENT SECURITY SOLUTION FOR MANET

Table 1. Comparison of existing methods and remarks

S. No	Author	Paper Title	Method / Algorithm	Year	Remarks
1	Ali Dorri	An EDRI-based approach for detecting and eliminating cooperative black hole nodes in MANET	Extended Data Routing Information Blackhole attack Detection	2016	Cannot detect the co-operatively blackhole attack node.
2	Gayathri Dhananjayan	T2AR: trust‐aware ad‐hoc routing protocol for MANET	extension trust-aware ad-hoc routing protocol	2016	locational information update-based trust rate computation takes more bandwidth.
3	Nadav Schweitzer	Contradiction Based Gray-Hole Attack Minimization for Ad-Hoc Networks	Denial Contradictions with Fictitious Node Mechanism	2017	detection of attacks and not their prevention and overhead are high.
4	Neelam Janak Kumar	Trust Value based Algorithm to Identify and Defense Gray-Hole and Black-Hole attack present in MANET using Clustering Method	Trust Value based Algorithm	2018	High power consumption under cluster-based routing.
5	R C Poonia, et., al.,	CDRA: Cluster-based dynamic routing approach as a development of the AODV in vehicular ad-hoc networks	cluster-based dynamic routing approach	2015	High consumption of energy with the requirement of low bandwidth for such type of network.
6	S. Hazra, et., al.,	Black Hole Attack Defending Trusted On-Demand Routing in Ad-Hoc Network	trusted approach to on-demand routing to defend blackhole attacker.	2014	discarded from route discovery packets by attacker.
7	S. Jain, et., al.,	Advanced Algorithm for Detection and Prevention of Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks	monitored independently at the neighborhood of both source and destination.	2010	This algorithm does not overhear each other's' received and transmitted packets some time normal node misbehaved.
8	A.Siddiqua, et., al.,	Preventing Black Hole Attacks in MANETs Using Secure Knowledge Algorithm	neighbor regarding packet operation	2015	Each node checking operation making it difficult to detect. It takes more time.
9	N.Choudhary, et., al.,	Preventing black Hole attack in AODV using timer-based detection mechanism	Route request (RREQ) sent by source node.	2015	Processing delay so timer-based check some time old packets of RREQ
10	Ashish Kumar Jain, et., al.,	Mitigating the effects of Black hole attacks on AODV routing protocol in Mobile ad-hoc Networks	SAODV	2015	High packet loss percentage.
11	Hinge, R., et., al.,	Opinion based trusted AODV routing protocol for MANET	trust calculation & opinion evaluation	2016	consuming the communication bandwidth in the network or memory space at individual nodes
12	Shah, S. N, et., al.,	A trust-based scheme against Packet dropping attacks in MANETs	Trust Based Secure Routing	2016	packet forwarding high energy consumption.

VI. CONCLUSION

MANETs is an emerging research area in modern life. In this paper we discussed about various routing protocols and issues of security in MANET. In existing security routing algorithm there is no proper attack detection algorithm implemented. so, it is likely to improvement various advantages by malicious behaviour users. The propose co-operating techniques to improve the malicious attack detection node. The economic benefits by exploiting incentive measures or exchange confidential information; saving power by selfish conduct; preventing somebody else from receiving proper service, extracting data to get confidential information. Furthermore, overcoming methods and different attacks in MANET are evaluated and analysed.

REFERENCES

[1] Ali Dorri "An EDRI-based approach for detecting and eliminating cooperative black hole nodes in MANET", Springer Science Business Media New York 2016.

[2] Gayathri Dhananjayan and Janakiraman Subbiah, "T2AR: trust‑aware ad‑hoc routing protocol for MANET", Springer Plus (2016) 5:995.

[3] Nadav Schweitzer, Ariel Stulman, Member, Asaf Shabtai and Roy David Margalit "Contradiction Based Gray-Hole Attack Minimization for Ad-Hoc Networks", in: IEEE Transactions on Mobile Computing, Volume: 16 Issue: 8, 2017.

[4] Neelam Janak Kumar Patel, Dr. Khushboo Tripathi, "Trust Value based Algorithm to Identify and Defense Gray-Hole and Black-Hole attack present in MANET using Clustering Method", IJSRSET, Volume 4, Issue 4, 2018.

[5] R C Poonia, D. Bhargava, and B.Suresh Kumar. "CDRA: Cluster-based dynamic routing approach as a development of the AODV in vehicular ad-hoc networks", In Signal Processing and Communication Engineering Systems (SPACES), 2015 International Conferenceon, pp.397-401. IEEE, 2015.

[6] S. Hazra, and S.K. Setua. "Black Hole Attack Defending Trusted On-Demand Routing in Ad-Hoc Network", In Advanced Computing, Networking and Informatics-Volume 2, pp.59-66. Springer International Publishing, 2014.

[7] S. Jain, M. Jain, H. Kandwal, "Advanced Algorithm for Detection and Prevention of Cooperative Black and Gray hole Attacks in Mobile Ad-hoc Networks", Intl. Journal of Computer Application 1(7): 37-42, Feb. 2010.

[8] A.Siddiqua, S.Kotari, and AAKhan Mohammed. "Preventing black hole attacks in MANETs using secure knowledge algorithm", Signal Processing and Communication Engineering Systems (SPACES), 2015 International Conferenceon. IEEE, 2015.

[9] N.Choudhary and L.Tharani. "Preventing black Hole attack in AODV using timer-based detection mechanism", Signal processing and communication engineering systems (SPACES), 015 international conferenceon. IEEE,2015.

[10] AK Jain and V Tokekar. "Mitigating the effects of Black hole attacks on AODV routing protocol in Mobile adhoc Networks", Pervasive computing (ICPC), 2015 international conference on. IEEE, 2015.

Authors Profile

I K. Sumathi had received M.Sc Computer Science at STC College, Bharathiar University from the Department of Computer Science, India, in 2013 wih gold medal. I had completed M.Phil Computer Science at Sree Saraswathi Thyagaraja College of arts & Science College, Bharathiar University in the Year 2014. I have 3.5 years of teaching experience. My area of interest are networking, Data Mining and Image Processing . Now I am pursing part time Ph.D in Computer Science under the guidance of D. Vimal Kumar.

D. Vimal Kumar received MCA degree at KSR College of Technology, Periyar University from the Department of Master of Computer Applications, India, in 2002. He received his M.Phil Computer Science degree at Kongu arts & Science College, Bharathiar University in the Year 2007. He received his doctorate in Anna University in the year 2014. He has 14 years of teaching experience. He is one of the approved supervisor of Bharathiar University currently guiding 06 scholars. He has published 17 articles in National /International journals. He has also presented papers in National and International Conferences. His area of interest includes data mining, network, software engineering, mobile computing and image processing. He is currently working as Associate professor in department of computer science in Nehru Arts and Science College, T.M Palayam, Coimbatore, Tamilnadu, India.