RESEARCHERID
THOMSON REUTERS

[*Saxena* et al., 4(6): June, 2017*] ISSN: 234-5197
Impact Factor: 2.715

INTERNATIONAL JOURNAL OF RESEARCH SCIENCE & MANAGEMENT

A RESEARCH ON ROUTING PROTOCOLS AND SECURITY OF CHALLENGES IN MANETs

Rajshree Saxena[*1] & Dr. Raghav Mehra[2]
[*1&2]Research Scholar, Bhagwant University, Ajmer
DOI: 10.5281/zenodo.583650

Keywords: Manet (Introduction), Routing, Protocols, Strategies, Security and MANET Challenges, Attacks on MANETs

Abstract
The procession in the area of internet due to wireless networking technologies gives rise to multiple new applications. In the past few decades, we have found many advance developments in wireless networks. With these developments and large number of applications that are being provided by MANETs, we still face some challenges that have to be overcome. The baseless and active nature of these networks demand new set of networking schemes that should be implemented to provide effective peer-to-peer communication. MANETs hire traditional TCP/IP structure to provide this peer-to-peer communication between nodes in the network. An important interesting research area in MANET is "Routing". This Routing is not only a very challenging task but also has received a rattling amount of attention from researches. Because of lack of a defined central authority, security of the routing process becomes a challenging task thereby leaving MANETs vulnerable to attempt, which results in declension in the performance as well as raises a serious question about the dependability of these such networks. In this paper, we are providing the history of MANET, challenges that are being involved in MANET and an overview of a spacious range of routing protocols proposed. We are also providing the known routing attacks and many of the proposed measures to these attacks in multiple works.

Introduction
MANET is a self configured mobile routers network which is connected by wireless links which do not have any access point. Every mobile (movable) device in any network is self directed. These devices are free to move indiscriminately. It states that an ad hoc network do not trust on any fixed sub structure or infrastucture. The Communication in MANETs is conducted by using multi-hop paths. Breaking down of communication link in MANET is very patronize because nodes can move anywhere. The number and density of nodes depend on the applications in which MANETs are used.

Routing in MANETs
"Routing" is the procedure to exchange information between various hosts in a network using most efficient path. Efficiency of path can be measured in various metrics like, Number of hops, traffic, security of MANETs etc.

Different Strategies of MANETs
Ad-hoc network Routing protocols can be classified into following strategies.

1. Flat architecture V/s Hierarchical architecture.
2. Pro-active routing protocol V/s Re-active routing protocol.
3. Hybrid protocols.

Flat V/s Hierarchical architecture
The term "Hierarchy" means tree like structure. Hierarchical network consists of multiple layers like a tree's branches in which top layers are of seen as the master of their lower layer nodes. In this architecture, there present many bunches of nodes and one gateway node among all the bunches which has the responsibility to communicate with the gateway node of the other bunch. In this scheme, there is a clear distribution of the tasks. This architecture breaks down whenever there is a single node failure i.e the Gateway node.

Proactive V/s Reactive routing protocol-

In proactive routing protocol all the nodes continuously maintain complete routing information about the network. This is done by the flooding of network sporadically with network status position to find out any possible changes in the network topology. Examples of Proactive Routing Protocols are

i) Global State Routing (GSR).
ii) Hierarchical State Routing (HSR).
iii) Destination Sequenced Distance Vector Routing (DSDV).

i) ***Global state routing (GSR)*** **-** The GSR protocol is based on the Link State algorithm. GSR has superclarified the way in which the information is circularized in Link State algorithm by bounding the update messages between the intermediate nodes only. In this algorithm, each node maintains a link state table based on the updated information which is being received from neighbor nodes and sporadically exchanges the state of its link information with these neighbor nodes only. This reduces the number of control messages which are transmitted via network. Hence, the size of update messages is large and thus the size of the network also grows and they get more larger.

ii) ***Hierarchical state routing (HSR)*** **-** HSR is also based on the traditional Link State algorithm like GSR. Unlike the other link state based algorithms, HSR maintains a hierarchical addressing map. Here, clustering algorithm is used to develop the nodes which have close propinquity with clusters. Each of the cluster has following types of nodes. They are-

*** Cluster-head node**: It acts as local coordinator for every node.
*** Gateway nodes:** These are the nodes that lie in two dissimilar clusters, and also
*** Internal nodes:** They are the other nodes in every cluster.

All nodes have their unique ID, which is called as the MAC address for each node. The nodes in each cluster broadcastly share their link information to each other.

iii) ***Destination-sequenced distance vector (DSDV)*** **-** *The* DSDV algorithm guarantees loop free routes. It provides a single path from the source to the destination. This path is selected by using the distance vector shortest path routing algo. Two update packets are used to reduce the amount of overhead transmitted network. These are termed as "full dump" and "incremental" packets. The full dump packet carried out the complete routing information and the incremental packet carried out the only information that has been changed since the last full dump. The incremental update messages are more frequent than the full dump.

In Reactive routing protocol, each and every node maintains information about only the active paths to the destination nodes. A search of route is required for every new destination therefore the communication overhead is decreased at the disbursal of delay to search the route. Speedily changing of wireless network architecture can break active route and can cause subsequent route search. Reactive routing protocols are more popular set of routing algorithms for mobile computation because they have low bandwidth consumption. Examples of reactive protocols are:

i) Ad hoc On-demand Distance Vector Routing (AODV).
ii) Dynamic Source Routing (DSR).
iii) Location Aided Routing (LAR).

i) **AODV:** AODV is distance vector routing where it does not involve nodes to maintain routes from the source to the destination that are not on active path. AODV does not play its part until end points are valid. Various route messages like Route Request (RREQ), Route Replies (RREP) and Route Errors (RERR) are being used to invent and maintain links. In AODV, a route with

maximum sequence number is selected. To find this new route the source node sends Route Request message to the network until it reaches the destination and then Route Reply is sent back to the source node. The nodes which are on active route interact with each other. If a node does not receive any reply then it deletes the node from the list and sends Route Error to all the members in the route.

ii) **DSR:** DSR is an On-demand source routing protocol, means here, the route paths are invented after a packet is sent to a destination node by the source in the MANETs. When initially the first packet is sent, the source node does not have any path to the destination. There are two functions of DSR first is "route discovery" and the second is "route maintenance".

Various caching techniques used in DSR: Each host which participate in MANETs maintain a route cache in which it caches the source route. There are many techniques for a node to learn & store the route, some of these are - Running network interface in sluttish mode, Reading the information of route from data packets and Reading the routing information from Route Discovery packets

iii) **Location Aided Routing (LAR):** LAR uses the flooding algorithm which is being defined in DSR. It has the exception that it uses location information of a specific node to fix the flooding of the network. This location information can be collected by using the Global Positioning System (GPS). When Some times the GPS can only give the approximate location of a node, even then also the LAR protocol can be used. By the use of location information, LAR can calculate the "expected zone" of that particular node.

Expected Zone: In a MANET, the expected zone is the area in which a particular node is expected to be at that particular moment.

Request Zone: LAR fixes the flooding using the request zone, that means in LAR, a node forwards a packet if it is in the request zone and cast out the packet if it is not in the request zone. A request zone must include the expected zone of the destination.

Hybrid routing protocols in MANET

Hybrid routing protocol is the fusion of both "Pro-active" and "Reactive protocols" in a MANET. In this protocol, there exists a number of routing

MANET Challenges

In mobile ad hoc networks, after the long history and huge development there are still some issues and challenges that we have to overcome. MANET is a self-organised wireless network of mobile nodes. In MANETs each and every device communicates with every other device. Following are the challenges in MANETs that we have seen

1. The scalability is required in MANETs because it is being used in military communications, as the network grows according to the requirement, hence every mobile device should be capable of handling the intensification of network and to fulfill the tasks.
2. MANETs are the infrastructure less network which has no central governance. Every device communicates with every another device, therefore it becomes very difficult to find out and manage the faults. As the mobile devices move randomly in a network of MANETs dynamic topology results in route changes and frequent network partitions.
3. MANETs are the autonomous networks, hence they have the tools for radio interface with different transmission receiving and sending abilities which results in asymmetric links. MANETs do not use any router for transmission.

4. In MANETs every single node acts as a router and forward the data packets another nodes providing the information among the mobile nodes. The MAC address of the device is being used in the stand alone ad hoc network.

Attacks In MANETs

All the routing protocols depend on active cooperation of nodes or active participation of nodes and to invent and access the network. The basic supposition in this kind of setup is that all the nodes are very well behaving and reliable. Due to dynamic and distributed infrastructure less behavior of MANETs, they are weak to different types of attacks. The challenges that are being faced in MANETs are above to those that are being faced by the traditional wireless networks. There are two types of attacks found in MANETs- "Passive Attacks" and "Active Attacks'. The availability of the wireless channel to both the genuine user and also the attacker makes the MANET available to active harmful attackers. Mobility of Nodes make the network topology dynamic forcing frequent networking configuration changes which create so many chances of attacks on MANETs. In passive attacks, the attackers do not send any of the message, but only listen to the channel. Passive attacks are information seeking. Active attacks can be directed to break up the normal node operation or can target the whole network operation. A passive attacker listens to the packets which contain the secret informations like IP addresses and location of nodes etc. that can be stolen, which removes confidentiality. It is normally not possible to detect this kind of attack in a wireless environment, because it cannot invent any new traffic in the network. An example of passive attacks is Eavesdropping. Since the wireless connections are present in MANETs, any of the message which is posted by any node could be listened by all nodes inside the network, and if there is no action like this then the attacker could get any type of valuable information provided by the sender node. Many authors has examined the danger of eavesdropping as a function of the broadcast range of the nodes. Active attacks can create disturbances in the procedures of the network and could be so severely bring down the whole network.

Conclusion

MANET is a rising technological area and hence is also an active area of research. Because of the features like ease of deployment and defined infrastructure less behavior these networks find uses in a variation of scenarios starting from emergency operations and disaster relief to military services. Providing security in such areas is very vital. Future research endeavor should be focused on improving the security effectiveness of the implemented schemes and on reducing their cost to make them suitable for a MANET environment. MANETs are gaining more and more solid base in the wireless communications. Whenever the application increases rapidly, the threats and security issues also increase in a network. Insecure wireless networks in a MANET are of no use. In this paper, we have introduced a short review of the most common widely generated threats and attacks. A few types of attacks on MANET are being presented. We have also found that Active attacks can be considered more dangerous because they break down the proper working operation of the MANETs. Passive attacks are not so harmful because of their standalone attacks. Research in MANETs protection is broaden as the sources of threats are broaden. The creation of a trust-based system can be done with the help of a good direction in research in which the type and diversity of security procedures applied trust on the level of rely

References

[1] Conti, Marco, and Silvia Giordano. "Multihop ad hoc networking: The reality."Communications Magazine, IEEE 45, (2016).
[2] Burbank, Jack L., Philip F. Chimento, Brian K. Haberman, and William T. Kasch. "Key challenges of military tactical networking and the elusive promise of MANET technology." Communications Magazine, IEEE 44, (2016).
[3] Marina, Mahesh K., and Samir R. Das. "On-demand multipath distance vector routing in ad hoc networks." 2015.
[4] Computer Engineering and Intelligent Systems (Paper) ISSN 2222-2863 (Online), 2015.
[5] In Advanced Communication Control and Computing Technologies (ICACCCT), 2014 International Conference IEEE, 2014.

[6] Pinnaka, A. K., D. Tharashasank, and V. S. K. Reddy. "Cost performance analysis of intrusion detection system in mobile wireless ad-hoc network." In Advance Computing Conference (IACC), 2013 IEEE
[7] Mafra, Paulo M., Joni da Silva Fraga, and Altair Olivo Santin. "Distributed IDS for Ad Hoc Networks." In Advanced Information Networking and Applications Workshops (WAINA), 2012.
[8] Ramrekha, Tipu Arvind, and Christos Politis. "A hybrid adaptive routing protocol for extreme emergency ad hoc communication." In Computer Communications and Networks (ICCCN), 2010
[9] Nadeem, Adnan, and Michael Howarth. "Adaptive intrusion detection & prevention of denial of service attacks in MANETs." In Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing 2009.
[10] He, Ting, Ho Yin Wong, and Kang-Won Lee. "Traffic analysis in anonymous MANETs." In Military Communications Conference,IEEE, 2008.
[11] Eichler, Stephan U., "Challenges of Secure Routing in MANETs: A Simulative Approach using AODV-SEC", IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS) Oct. 2006.
[12] Basagni, Stefano, Marco Conti, Silvia Giordano, and Ivan Stojmenovic, "Mobile ad hoc networking", 2004.
[13] B. Bellur, R.G. Ogier, F.L Templin, "Topology broadcast based on reverse-path forwarding routing protocol" , 2003.
[14] S. Das, C. Perkins, E. Royer, "Ad hoc on demand distance vector (AODV) routing", 2002.
[15] In Network Protocols, 2001." Ninth International Conference on, pp. 14-23. IEEE", 2001.