WWJMRD 2017; 3(11): 376-378
www.wwjmrd.com
International Journal
Peer Reviewed Journal
Refereed Journal
Indexed Journal
UGC Approved Journal
Impact Factor MJIF: 4.25
e-ISSN: 2454-6615

Niharika
Student, Yadavindra College of Engineering, Punjabi University, Guru Kashi Campus, Talwandi, India

Manoj Kumar
Assistant Professor, Yadavindra College of Engineering, Punjabi University, Guru Kashi Campus, Talwandi Sabo, Punjab, India

Correspondence:
Niharika
Student, Yadavindra College of Engineering, Punjabi University, Guru Kashi Campus, Talwandi, India

A Review on Different Types of Attacks in MANET

Niharika, Manoj Kumar

Abstract
MANET is Mobile ad-hoc network. It includes large number of wirelessly connected nodes. This type of network is also called as peer to peer network. It is infrastructure less network, have large number of vulnerabilities. Those are like malicious node attack, congestion, or hardware failure. Due to these problem this network can be an unsecured network. Various researchers has emphasis on detection and mitigation of different types of attacks and there management technique. MANET because is low cost network, various researchers has emphasis on techniques which works at network layers level, rather than at hardware level. So large amount of work still can be done in the field of security. So that the reliability of the network can be further enhanced.

Keywords: MANET, Routing attack, Security.

Introduction
Mobile ad-hoc network is a network which consists of two or more nodes, moves in short area. They moves with different speeds. While moving with different speeds they do communicates to each other. While communication one source node identifies the path to the destination node through routing protocol. When two or more node in direct radio range of each other, then communicates to each other directly. But if they are not in direct radio range to each other they identifies the path by considering another intermediate node. Through this intermediate node source node arrives at the destination. While connecting from source to the destination they identifies the route using different types of routing protocols like reactive (AODV) and proactive (OLSR) or Hybrid (ZRP) etc.

1.1 Attacks classification
There are various types of attacks in the network due to which network efficiency alter significantly. These attacks can be of various nature like internal attacks, External attack, Active attacks, and Passive attacks. Each type of attacks have different types of effects on the network performance. So each type of attack need to be studied.

1. External Attack: This type of attack is by the node does not belongs to the legitimate node list. This attacker node which belongs to the outside access into the network illegally. Once this node become part of the network can destroy the network performance by sending large number of unnecessary packets. So these type of malicious nodes need to be addressed timely [15].
2. Internal Attacks: This kind of attack is due to the misbehavior of the node which is part of the network, but due to certain reason it started behaving in false way. Such that starts destroying the network. In results network performance will be downgraded [15].
3. Passive attack: This type of attacker node does not destroys the network performance, but rather keep track of data or listen to the data transferred between two node source and destination. This type of attack otherwise does not degrades the performance, but destroys the integrity of the network [15].
    a. Eavesdropping: In this type of attack attacker listens to the data being transferred between two parties. By reading the data it can extract the useful data like password, account number etc[13][15].

b. Traffic analysis: In this type of attack attacker node sees the traffic both incoming to the node or outgoing from the node. So that traffic pattern can be identified [15].

4. Active attack: In this type of attack attacker node actually become part of the communication and starts destroying the packets and even starts miss-route the packets [15].

There are various types of active attacks like.

a. Black Hole Attack: This type of network works at Network layer. It is the hostile node which work in bad intension. When certain bad node send the route request, these black hole nodes will be the first node to reply for having true destination address. Such that source sends all the data packets to this intermediate node. But it rather than forwarding the data packets will drops the data packets. And forward the false packets. In bottom they deteriorate the network performance [13][15].

b. Warm Hole Attack: Warm hole attack is the most performance reducer type of attack. In this warm hole node tunnels the data packet to another route. This type of attack misroute the data packets. By misrouting the network traffic will be increased and also large amount of energy will be wasted while transmitting the data packet from source to the destination [15].

c. Sleep Derivation Torture Attack: This type of attack works at layer 2. In this type of attack extra control bits are attached to data packet. This process will continues till the all nodes which are part of the communication get exhausted or destroyed [13].

d. Jellyfish Attack: This type of attacker includes attacker node which first tries to get access to the network. Once it will get the access to the network will put unnecessary delay into the network. As a result unnecessary end to end delay will be increased [15].

e. Misrouting Attack: This type of attacker node works in selfish way. Any data packets which are originating from certain source for specific destination will be misrouted towards another false destination [13][15].

f. Sybil Attack: This type of node which work as attacker node will be generating the copy of another node and starts behaving in another legitimate node. This way it behaves as attacker node and destroys the network traffic [15].

g. DOS Attack: In this type of attack attacker node sends the millions of false data packet on the server. It will overload the whole network. That means server will be busy in processing large number of false packets [15].

1.2 Various Attacks and There Prevention Technique

Table 1. Comparative table of all techniques

Author	Paper name	Technique	Constraints
[1] Srinivas Aluvala	An Empirical Study of Routing Attacks in Mobile Ad-hoc Networks	Technique used for Identification is SAODV.	This technique does not recover from attack situation
[4] Leovigildo Sanchez-Casado	Identification of contamination zones for sinkhole detection in MANETs	This paper uses ack. Method, based on time threshold to detect the sink hole attack.	This techniques does not provide full proof system.
[5]Gayatri Wahane	Technique for Detection of Cooperative Black Hole Attack using trust based path in Mobile Ad-hoc Networks	This paper focus on the process of identification of co-operative black hole attack. It identifies the attack using trust based technique	While identification of the cooperative black hole attack the performance still can be further enhanced.
[9] U. Venkanna	Security Threats In MANETs: A Review	This paper has put the technique based on trust based mechanism.	This technique can be further enhanced with other types of attacks like overflow attacks
[6] Kavitha Subramaniam	Efficient Buffer Management Protocol for Multicast Streaming in MANET	This paper is based on buffer management at the node level while there is multicasting streaming in the network	This technique can be further enhanced by having thresholding on to the buffer at each node.
[2]Vijay Laxmi	JellyFish attack: Analysis, detection and countermeasure in TCP-based MANET	proposed a light-weight direct trust-based detection (DTD) algorithm which detect and remove a Jelly Fish node from an active Communication route.	This technique can be enhanced to other type of attacks.
[3] Jefin Liza James	A Study on Preventing Node Isolation Attack in OLSR Protocol	This paper has proposed a study for different type of attacks for proactive protocol OLSR.	This type of technique is very hard to follow when there is no rule broken for protocol.
[7] Mohamed elboukhari	Analysis of the security of bb84 by model Checking	The Prism tool to analyze the security of bb84 protocol and we are focused on the specific security property Of eavesdropping detection.	Automatic model checker prism enables them to analyze bb84 protocol more efficiently.
[10] Harshavardhan Kayar	A Survey on Security Issues in Ad Hoc Routing Protocols and their Mitigation Techniques	survey the common security threats and attacks and summarize the solutions Suggested in the survey to mitigate these security vulnerabilities.	Comparative analysis of different techniques that are employed to mitigate diverse security.

Literature Review

Srinivas Aluvala (2016) et al more focused on security issue of ad-hoc networks and solution to mitigate such attacks using SAODV Based technique.

Vijay Laxmi (2014) et al. Focused on attacks mitigation and by using light-weight direct trust-based detection (DTD) algorithm the attack will be mitigated. So that perfor- mance can be enhanced.

Jefin Liza James (2016) et al According to the researcher there was denial of service attack. By using node isolation technique this type of attack can be detected and removed.

Sanchez-Casado (2016) et al. had discussed the concept of border node. Using border node sink hole attack can be mitigated. The protocol on to which they have worked upon is OLSR (Optimized link State Routing protocol.

Gayatri Wahane (2014) et al: Trust based technique can be used for identifying the path through which there was a communication. So that more reliable path can be established. Using true link technique various kinds of attacks can be identified and removed timely so that network performance cannot be downgraded.

Kavitha Subramaniam(2014) Buffer at each node can be managed. This buffer will be used to store the packets, so that packets can be transferred as non-real time data.

Mohamed Elboukhari (2010) et al. the

PRISM tool to analyse the security of BB84 protocol and we are focused on the specific security property of eavesdropping detection. Precisely, we use the PRISM tool to analyse the security of BB84 protocol and we are focused on the specific security property of eavesdropping detection. We show that this property is affected by the parameters of quantum channel and the power of eavesdropper.

Harshavardhan Kayar(2012) et al. Discussed different ad hoc routing protocols, explained the working of each and provided a table that lists the ad hoc routing protocols and the properties exhibited by each of them. In the next section we listed various security vulnerabilities and threats that are encountered in the MANETs. We explained each of the security threats and the effects they cause on the ad hoc networks. In the last section we discussed several techniques to mitigate the security threats and attacks listed in the previous section. We categorized the solutions based on various techniques.

Conclusion

Various researcher in different research paper MANET is called to be most vulnerable network. Any node which is the part of the network or not the part of the network can attack on to the network. These attacks can be both active attacks and passive attacks. Active attacks downgrades the performance of the network because they directly starts participating in the communication either by declaring themselves as intermediate node or misroute the traffic. But passive attacks does not destroys the network performance but reduces the network integrity by sniffing the secured information like password or account number. There is always a requirement of identifying the attacker node and protecting the network. According to different researcher point of view every time network is having risk of new kind of security risk. There requires continuous research in the field of protection with different means. So that network resources should not depleted fast.

Future Work

Current review has been done on the various types of attacks. These attacks can be in category of both active and passive. In future routing attack can be researched so that MANET can be secured from this type of attacks and performance can be enhanced.

References

1. Srinivas Aluvala, Bhubaneswar,"An Empirical Study of Routing Attacks in Mobile Ad-hoc Networks",Procedia Computer Science vol. 92, pp. 554–561, 2016.
2. Vijay Laxmi, Chhagan Lal, M.S. Gaur, Deepanshu Mehta, "JellyFish attack: Ana- lysis, detection and countermeasure in TCP-based MANET", Procedia Computer Science, Vol. 4,pp:321-329. 2014.
3. Jefin Liza Jamesa, Bino Thomas, "A Study on Preventing Node Isolation Attack in OLSR Protocol", Procedia Technology,Elsevier, vol.25,pp:349 355, 2016.
4. Leovigildo Sanchez-Casado, Gabriel Macia-Fernandez, Pedro Garcia-Teodoro, Nils Aschenbruck, "Identification of contamination zones for sinkhole detection in MANETs", Procedia Computer Science, vol. 3, pp: 123-34, 2015.
5. Gayatri Wahane, Ashok M. Kanthe, Dina Simunic, "Technique for Detection of Cooperative Black Hole Attack using True-link in Mobile Ad-hoc Networks", Procedia Computer Science vol. 3, pp:26-30,2014.
6. Kavitha Subramaniam, Latha Tamil-selvan, "Efficient Buffer Management Protocol for Multicast Streaming in MANET", IJSRD, vol. 3,pp: 222 – 232,2014.
7. Mohamed Elboukhari, Mostafa Azizi and Abdelmalek Azizi, "Impact Analysis of Black Hole Attacks on Mobile Ad-hoc Networks Performance", IJSET, Vol.6, pp:1-11, 2015.
8. Aarti Chauhan, Puneet Rani, "A Detail Review of Routing Attacks in Mobile Ad-hoc Networks", Procedia Computer Science, Vol. 3, pp: 1154-1163, 2015.
9. U. Venkanna ,Shikha Jain, "Security Threats In MANETs: A Review", Procedia Computer Science ,Vol. 3, pp: 37-50, 2014,
10. Harshavardhan Kayarkar, "A Survey on Security Issues in Ad-hoc Routing Protocols and their Mitigation Techniques", IJRECE, Vol. 03, pp: 1338-1351, 2012.
11. Nitish Balachandran, "Surveying Solutions to Securing On-Demand Routing Protocols in MANETs", IJRCST, Vol.:04, pp: 1486-1491, 2012.
12. Ashwani Garg, Vikas Beniwal, "A Review on Security Issues of Routing Protocols in Mobile Ad-Hoc Networks", Procedia Computer Science, Vol. 2, pp: 145-148, 2012.
13. Dr.R.Satyaprasad, Dr. K. Raja sekhara rao, "A Survey on Attacks and Defense Metrics of Routing Mechanism in Mobile Ad-hoc Networks", Procedia Computer Science, Vol. 2, pp: 7-12, 2011.
14. Praveen Joshi, "Security issues in routing protocols in MANETs at network layer",IJSCE,vol. 3, pp:954–960, 2011.
15. Pooja Chahal, Gaurav Kumar Tak, Anurag Singh Tomar, "Comparative Analysis of Various Attacks on MANET", Procedia Computer Science, Vol. 111, pp: 42-50, 2015.