IJCSN - International Journal of Computer Science and Network, Volume 8, Issue 2, April 2019
ISSN (Online) : 2277-5420
www.IJCSN.org
Impact Factor: 1.5

Comparative Analysis of Attacks and Countermeasure in MANET

[1] Puneet Kamal; [2] Rajeev Sharma; [3] Abhishek Gupta

[1]M.Tech (Research Scholar), [2] Assistant Professor [3] Assistant Professor
Chandigarh Engineering College, Landran, Mohali, India

Abstract-Security is a key issue to ensure protected communication between mobile intersections in adversary environments. Unlike cable networks, it creates some non-leakage issues, such as the unique features of mobile ad hoc networks (MANETs), secure peer-to-peer network architecture, shared wireless interference, harsh resource restrictions, and high dynamic network topology. These difficulties create a hub for creating a multifunctional security solution to achieve extensive protection and performance of any network. In this article, we pay attention to the main security problem of MANET. We identify security issues with the discussed issues a security design is also discussed. A review of the latest security recommendations for MANETalong with the performance is discussed.

Keywords- MANET, Routing, Security Criteria, Attacks, Security solution.

1. Introduction

The Mobile Ad hoc Network (MANET) is a wireless network for portable computing devices without the support of any fixed infrastructure. Mobile nodes in MANET are self-organizing. These networks can be applied between vehicles between people or between areas where the fixed infrastructure is exhausted. These areas may be military battlefields or some flood or earthquake-stricken areas [1]. If two nodes are in the radio range, they can communicate directly with each other. If the nodes are not in the radio range, they can communicate with each other using multi-hop routing.

The general structure of MANET is shown in figure 1, which consists of a number of mobile nodes denoted by a circle. The source and the destination node is represented by the red and the green colour respectively. Every node has its own communication range and the nodes that have the same communication range come under the same cluster as shown in figure 1. The figure comprises four clusters and each cluster is operated by a cluster head before communication to the base station and is denoted by the yellow circle. Therefore, whenever the node wants to transmit data, it first communicates with its cluster head [2].

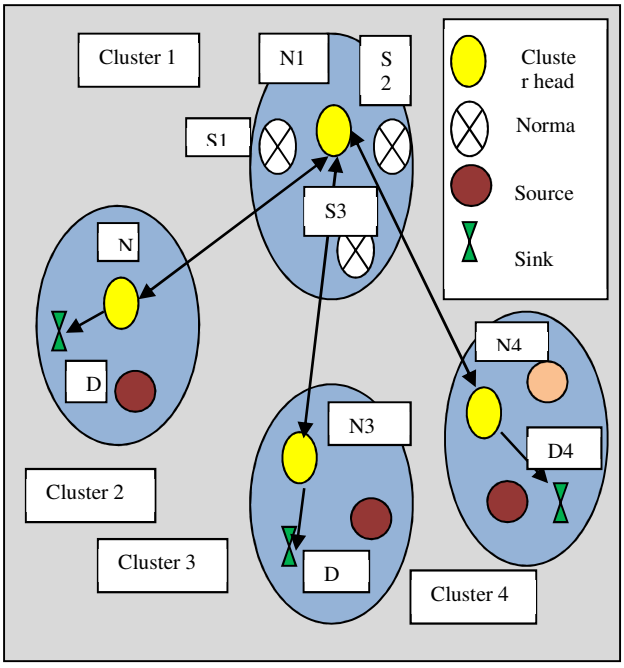

Fig.1 General Architecture of MANET

Cluster head checks the destination address inits data packet, if the destination is within the cluster then forward data to the destination. Otherwise, cluster head, communication with its neighbouring cluster head. In this way, the data is routed to its destination node [3].

For the transmission of data, there isa number of routing protocols that are available. A brief description is provided in table 1.

Table 1: types of routing [4]

Routing Types	***Definition***	***Example***
Proactive	It utilized link state routing mechanism that often floods information about their nearby nodes. It maintains routing information and keeps track of the control pack with neighbours up to date.	Destination-Sequenced Distance Vector (DSDV) and Optimized Link State Routing (OLSR)
Reactive	The problem of routing overhead is resolved in reactive routing. It employs the distance-vector routing algorithm and creates the route to be specified when a node is required by starting the route discovery process.	Ad-hoc On-demand Distance Vector (AODV) and Dynamic Source Routing (DSR)
Hybrid	It is a combination of reactive and proactive routing protocols	Zone Routing Protocol

The MANET has the following features as defined below:

1. Wireless connections among nodes are very sensitive. The reason is that as the nodes are moving frequently and cause link breakage. Also, the power provided to the nodes is limited.
2. The topology of the network is very dynamic because of continuous disruption and wireless connection as the nodes enter and exit from their communication rage very rapidly. This causes the routing information to change.
3. Bandwidth is limited on these wireless networks.
4. MANETS needs energy-efficient work because all the intersections are dependent on a battery that is highly empowered [5].

These features show that MANET needs a secure operation. Current routing protocols do not pay much attention to security aspects. MANETs are more vulnerable to security threats than the traditional cable network. In this article, security issues are investigated, and some methods of protecting the network from different threats are also discussed to achieve security [6].

Table 2: Security Criteria in MANET [7]

Security measure	***Description***
Availability	Regardless of the network status, it refers to the network's services provided to the users. Denial of service (DoS) attacks based on availability criteria.
Integrity	This feature guarantees that there is no modification in the message is allowed as it may be malicious or accidental.
Confidentiality	This message indicates that an unauthorized person cannot even read the original information.
Authenticity	With this property, the participants prove their identity. This property makes sure that the participants are unrealistic.
Non-repudiation	Using this feature of MANET the sender and the receiver cannot refuse to send and receive the message.
Authorization	This property gives multipleaccesses to various types of users. For example, network management can be done by the network administrator.
Anonymity	Entire information related to the identity of a node should be kept confidential for confidentiality.

2. Attacks in MANET

MANET attacks can be external or internal. External attacks cause clogging, sending incorrect routing information or causea lack of services. In an internal attack, the malicious node from the network receives unauthorized access and behaves like a real node. It can analyze traffic between other intersections and participate in other network activities.

Table 3: MANET Attacks [8-10]

Attack Type	***Description***
Denial of Service attack	It affects the existence of a single node or the whole network. If the attack succeeds, the services will not be accessible by the end user. This attack mainly utilized radio signal jamming as well as battery exhaustion mechanism.
Impersonation	When a validation mechanism is not properly put into practice, a malevolent node can act as a node and control network traffic. It can also send fake routing packages and access some secret data.
Eavesdropping	This is a passive attack. The node simply monitors hidden data. This information can then be utilized by the malicious node. Confidential information, such as location, public key, personal key, password, etc. might be fetched by the eavesdropper.
Routing	The malicious node becomes a target

Attacks	for routing services because it is an essential service in MANET. There are two types of attack composed by this type. One attack on routing protocol, packet transfer or delivery mechanism attack to another. The first is to prevent routing information from spreading to a node. The latter worries the delivery of the package to the predetermined route.

3. Security Solutions in MANET

In this section, we explore a few security schemes to deal with attacks described in the preceding sections.

Table 4: Security Solution in MANET

Security techniques	***Description***	***Existing work***
Intrusion Detection	An IDS is a system that observes network traffic for doubtful activity and provides alarms when such activity is detected.	Shams, E. A., &Rizaner, A. (11, 2018) have proposed a hybrid approach of IDS with Support vector machine (SVM) to identify DoS attack in MANET. The attack is detected with a detection rate of approximately 95 %. Sen et al. (12, 2018) have presented a trust model that behaves similar to IDS and utilized for the detection of black hole attack in MANET. 20931 Kbps throughput with a delay of 2260ms has been achieved.
Cluster-based Instruction Detection	The distributed and cooperated IDS structure suffers from the lack of battery power as a few nodes behave like as a selfish node. To resolve this problem a cluster based IDS is developed, in which the entire network is divided into a group of clusters. Every node is the part of at least one cluster.	Ahmed et al. (13, 2006) have proposed cluster-based IDSutilized to identify intrusion with a high detection rate and less execution time. The detection rate upto 97 % has been achieved for Blackhole attack. Dang, N., & Mittal, P. (14, 2012) have designed cluster based IDS to restrict intruder activity in groups of mobile nodes. In clusters, each node launches a set of permissions to detect local and global intervention.
Defending Wormhole Attack using clustering scheme	In the Wormhole attack, the participants record and replays with another node through tunnels. For the receiver node, it becomes complex to differentiate between genuine and legitimate user.	Roy et al. (15, 2010) have employed a clustering scheme for the detection of wormhole attack in MANET. Raote, N. S. (16, 2011). Have contributed to the detection of wormhole attack in MANET.
Defending Man-in-the-Middle	Man-in-the-middle is a type of eavesdropping attacker that occurs when a malicious actor incorporates itself as a proxy/person in a communication session between a system and a system. Man-in-the-middle attacks real-time operation of transactions, conversations or other data transfer.	Sowah et al. (17, 2019) have proposed a detection and prevention algorithm against Man-in-the-Middle named as Artificial neural network with a detection rate of 88.235%.

4. Comparison of Existing Work

This section illustrates the comparison of the detection rate analyzed by various authors for the prevention of MANET from different types of attack.

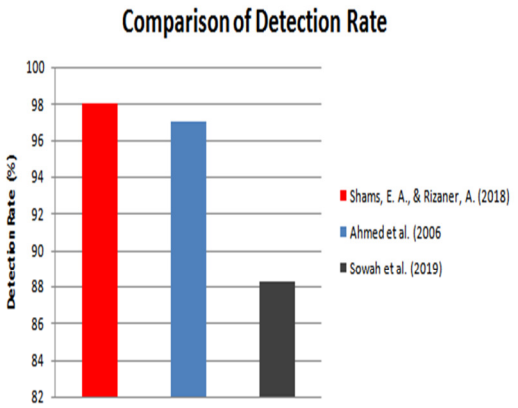

Fig. 2 Comparison of detection rate

Figure 2 represents the comparison graph for detection rate measured by different authors named as Shams, E. A., &Rizaner, A. (2018), Ahmed et al. (2006), and Sowah et al. (2019) respectively. From the graph, it is clear that detection ratemeasured by, E. A., &Rizaner, A. (2018) for the detection of DoS attack using IDS in addition with supervised learning scheme SVM in MANET is higher about 98 % compared to other existing techniques.

5. Conclusion

Due to the dynamic infrastructure of MANET that worked without centralized management, this kind of network is more vulnerable to many attacks. In this article, we discuss the security issues and the different types of routing protocols in MANET.An attempt was made to provide an overview of a few available security attacks in MANET.This network needs to be safer and strengthened to suit the requirements of the network. In this article, research on MANET safety is still a challenge and opens the door for researchers. Also, a comparison between existing prevention techniques has been performed. From the analysis, it has been observed that when an artificial intelligence technique is used with intrusion detection system the detection rate of the network has been increased.

References

[1] M. Usman, M. A. Jan, X. He, & P. Nanda, "QASEC: A secured data communication scheme for mobile Ad-hoc networks," Future Generation Computer Systems. 2018.

[2] I. Naz, S. Bashir, & S. Abbas, "Secure Routing in Mobile Ad hoc Network," Sukkur IBA Journal of Computing and Mathematical Sciences, Vol. 2, No. 2, 2018, pp. 14-21.

[3] A. K. Gupta, & S. Prakash , "Secure communication in cluster-based ad hoc networks: a review," In Next-Generation Networks , Springer, Singapore, 2018, pp. 537-545).

[4] F. Mohammed, C. Badr, & E. Abdellah, "Comparative study of routing protocols in MANET," In 2014 International Conference on Next Generation Networks and Services (NGNS) , 2014, pp. 149-153).

[5] P. Goyal, S. Batra, & A. Singh, "A literature review of security attack in mobile ad-hoc networks," International Journal of Computer Applications, Vol. 9, No.12, 2010, pp. 11-15.

[6] H. Sargolzaey, A. A. Moghanjoughi, & S. Khatun, "A review and comparison of reliable unicast routing protocols for mobile ad hoc networks," IJCSNS International Journal of Computer Science and Network Security, Vol. 9, No.1, 2009, pp. 186-196.

[7] O. O. Obi, "Security issues in mobile ad-hoc networks: a survey," The 17 th White House Papers Graduate Research In Informatics at Susse, 2004.

[8] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, & A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks," IEEE Wireless communications, Vol. 14, No. 5, 2007, pp. 85-91.

[9] M. C. Trivedi, Yadav, S., & Singh, V. K, "Securing ZRP Routing Protocol Against DDoS Attack in Mobile Ad Hoc Network,"In Advances in Data and Information Sciences , Springer, Singapore, 2019, pp. 387-396.

[10] P. M. Jawandhiya, M. M. Ghonge, M. S. Ali, & J. S. Deshpande, "A survey of mobile ad hoc network \ attacks.," International Journal of Engineering Science and Technology, Vol.2, No.9, 2010, pp.4063-4071.

[11] E. A. Shams, & A. Rizaner, "A novel support vector machine based intrusion detection system for mobile ad hoc networks," Wireless Networks, Vol.24, No.5, 2018, pp.1821-1829.

[12] B. Sen, M. G. Meitei, K. Sharma, M. K. Ghose, & S. Sinha, "A Trust-Based Intrusion Detection System for Mitigating Blackhole Attacks in MANET," In Advanced Computational and Communication \ Paradigms , Springer, Singapore, 2018, pp. 765-775 .

[13] E. Ahmed, K. Samad, &, W. Mahmood, "Cluster-based intrusion detection (CBID) architecture for mobile ad hoc networks," In 5th Conference, AusCERT2006 Gold Coast, Australia, May 2006 Proceedings.

[14] N. Dang, &, P. Mittal, "Cluster based intrusion detection system for MANETS," International Journal of Computer Applications & Information Technology, Vol.1, No.1, 2012..

[15] D. B. Roy, R. Chaki, & N. Chaki, "A new cluster-based wormhole intrusion detection algorithm for mobile ad-hoc networks," International Journal of Network Security & Its Applications Vol.1, No. 1, 2009, pp.44-52.

[16] N. S. Raote, "Defending wormhole attack in wireless ad-hoc network," International Journal of Computer

Science & Engineering Survey, Vol. 2, No. 3, 2011, pp. 143-148.

[17] R. A. Sowah, K. B. Ofori-Amanfo, G. A. Mills, & K. M. Koumadi, "Detection and Prevention of Man- in-the-Middle Spoofing Attacks in MANETs Using Predictive Techniques in Artificial Neural Networks (ANN)," Journal of Computer Networks and Communications, Vol. 2019, pp. 1-14.