International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 03 | Mar-2018 www.irjet.net p-ISSN: 2395-0072

Secure Data Transmission from Malicious Attacks: A Review

Anuradha T

Department of CSE, PDA College of Engineering, Kalaburgi, Karnataka, India

---

Abstract - *Secure transmission refers to the transfer of data such as confidential or propriety information over a secure channel. Many secure transmission methods require a type of encryption. Security is a main issue of the mobile ad-hoc network, because of ad-hoc property the newly node easily join or leave the network. While transmission from one node to another nodes establish a path with the help of intermediate nodes. Due to the mobility of nodes in the network the malicious nodes can be easily introduced in the network and the network can be compromised. Because of dynamic nature of the network it is important to maintain the security of the network. The performance of the network depends on the behaviour of the nodes. In this paper, the main focus is to study and analyse the different techniques and system proposed by the researchers for various attacks and detection for secure data transmission.*

Key Words: **MANETs, AODV, Security attacks, Cryptography techniques.**

1. INTRODUCTION

Mobile Ad-hoc Network (MANET) is a self-organized wireless network of mobile nodes without any fixed infrastructure. Nodes roam through the network, causing its topology to change rapidly and unpredictably over time. New nodes can join the network, whereas at the same time other nodes leave it or just fail to connect (temporarily) because they move to a region that is not in the cover range of the network. Nodes are typically wireless devices such as PDAs, laptops or cellular phones. From the very beginning, the use of MANETs has been appealing for both military and civilian applications, especially in the last decade because of development of wireless LAN technology. Due to their inherent characteristics of dynamic topology and lack of centralized management security, MANET is vulnerable to various kinds of attacks. These include passive eavesdropping, active interfering, impersonating, and denial-of-service. Malicious attack is one of many possible attacks in AODV-based MANETs. In this attack, a malicious node sends a forged route reply (RREP) packet to source node that initiates the route discovery in order to pretend to be the destination node. The standard of AODV protocol, the source node compares the destination sequence number contained in RREP packets when a source node received multiple RREP, it judges the greatest one as the route contained in that RREP packet. In case the sequence numbers are equal, it selects the route with the smallest hop count. As the result, the data transmission will flow toward the malicious node by source node and it will be dropped.

MANET is a network continuously self-configuring infrastructure-less network of mobile devices connected wirelessly that are composed of mobile devices or other mobile pieces, that can arrange themselves in various ways and operate without strict top-down network administration. Distributive and free autonomous node causes vulnerabilities to Denial of Service (DOS) attacks. Denial of service is any type of attack where the attacker attempt to prevent legitimate users from accessing the service. A Denial of service attack is when a attacker is trying to generate more traffic than you have resources to handle. Some security attacks are shown in Table 1., below are syn flood, black hole, sink hole, jellyfish attack etc...

Table -1: Security attacks in MANET

Security attacks	Description
Syn flood	Is a type of DOS attack in which an attacker sends a series of SYN requests to target's system in an attempt to use vast amounts of server resources to make the system unresponsive to legitimate traffic
Black hole attack	Is a problem that one malicious node utilizes the routing protocol to claim itself of being the shortest path to the destination node, but drops the routing packets but does not forward packets to its neighbours
Sink hole attack	Is the type of attack were compromised node tries to attract network traffic by advertise its fake routing update.

This paper describes the impact of security attacks and different techniques to control and avoid effect of various attacks in MANET and provide better security for secure data transmission.

2. RELATED WORK

To reduce such malicious activity without expensive cryptography they have given a new concept of Self Protocol Trustiness(SPT) in which detecting a malicious nodes and its activity is accomplished by the normal protocol behaviour and they have presented a Blackhole Resisting Mechanism (BRM) here not require expensive Cryptography or authentication mechanisms is discussed in [1] BRM_AODV is designed to mitigate the effect of the blackhole attack on the performance of AODV protocol by fast detection of blackhole neighbours. The mechanism introduces a new concept of self-protocol trustiness (SPT) the mechanism not use cryptographic techniques which conserves the power and

computation resources. BRM-AODV gives a huge improvement of the network performance in all metrics over both AODV and SAODV. The proposed mechanism succeeded in detecting blackhole nodes within a short time regardless the number of malicious node.

Based on the behaviour of nodes a mathematical theory of evidence that is Dempster Shafer theory for calculating the trust of nodes, this is a mathematical theory of evidence and a theory of behavioural reasoning. The degree of trust replace the evidence. Dumpster's rule of grouping is the way to aggregate and brief quantity of evidences D-S theory for calculating trust of nodes in MANET initially, all nodes have the same trust after that when communication start, D-S theory apply on the behaviour of nodes so that it calculate the trust probability of nodes in the network. The simulation result using D-S theory get better result in form of packet delivery ratio, throughput routing overhead of this work increase because of trust calculation happen again and again has been observed in [2]

For protecting wireless sensor network from DOS attack designed a new technique in [3] the main intension of this paper is to protect WSN from DOS attack design a dynamic forwarding window technique for securing the network from DOS attack. This scheme is on the basis of dynamic time, this time is known as forwarding window and it will be calculated in route request phase if any node floods the route request message more than forwarding window then it will detect as attacker. Forwarding window=Number of neighbours*(Time at which RREQ was received-Time at which RREQ was sent). Energy consumption is one of the parameter impacted by flooding attack, the same parameter showed an improvement of 7.14 percent as compared to the existing scheme. The Lessing of the flooding of the route request packets tends to consume lesser amount of energy on the part of the nodes then preserving the major resources of the network namely energy consumption, this is not only detected the malicious node but also succeeded in reducing the damage caused to the network by such malicious nodes. This type of attacks can be reduced by using AODV is a reactive routing in which each node maintains a routing table which contains the information about neighbour node from which the packets is arrived in order to search destination path. Experiments are performed on ns-3 simulator and calculated average End-to-End delay. Packet delivery ratio and routing overhead using AODV routing in the network a packet takes 0.3 milliseconds average time from source to destination node using AODV routing and overhead in the network happens with 83.33% when speed of node is increased in network packet delivery ratio is decreased due to increasing probability of link breaks among nodes the detecting technique do not guarantee of achieving 100% PDR as detection take some time duration and this time duration packets are dropped. In [5] implemented jellyfish attack in delay variance attack on AODV and proposed a JFDV detection algorithm that analyzes multiple JFDV attacker nodes it reduces average end-to-end delay and increase throughput by re-routing data packets through alternate route consisting of malicious nodes.

Security is a major aspect in MANET, there is need to heal performance of attack effected networks. Jellyfish delay variance attack introduce delay in the network and leads to decreased throughput. Detecting malicious node that performing malicious activity is one of the major concern.
To protect the data from modification the new improved technique is discussed in [6] for the detection of malicious node CONFIDANT is the one of effective technique but this is also incorporated with some weaknesses. This paper proposed a malicious node detection technique, called improved CONFIDANT technique which resolves significant problems of CONFIDANT techniques such as detection and prevention of blackhole nodes, false reporting problem, network collision as well as providing quality of service. This solves the significant problem of watchdog technique, detect malicious node from the innocent node. Solve the false reporting problem and deal with malicious node colluded in MANETS, CONFIDANT technique is an effective and efficient method to detect malicious node but is also associated with some weakness. This proposed work trying to remove these weaknesses and proposed a new technique improved CONFIDANT technique this reduces the number of packets drop and provides security against malicious nodes by isolating them from adhoc network it also reduces the false positive and false negative message to spread in the network. Improved CONFIDANT technique can be implemented to provide security against modification and fabrication of data packets by malicious node.

The gray hole attack has two improvement stages in first stage a malicious node exploits the AODV protocol to advertise itself as having a valid route to the destination node with intension of interrupting or corrupting packets in second stage nodes drop the interrupted packets. Even in the presence of large node numbers to maintain better performance of network is observed in [7] work about the implementation of a mechanism for detecting gray hole attack in MANET on AODV protocol. The aim of work is to develop secure adhoc demand distance vector routing protocol to detect grayhole attacks in MANET. In this work a gray hole attack has been detected in the networks to avoid any dangerous circumstance. This research work carried out a study and analysis of AODV routing protocol with various security threats it works for both static and mobile node, reduces End-to-End delay better performance for large node number.

Also multipath algorithm can be used for the same purpose to produce good packet delivery ratio they have proposed a packet update scheme and even advise the elimination scheme by discovering all malicious nodes multipath algorithm is used results in the restoration of average count of hops by excluding the attacker node from the original node. OPENET simulator is used. Packet delivery ratio and end-to-end delay decreases.

To protect the data from malicious node a latest cryptography technique is used In this work, a robust and scalable infrastructure based security overlay is designed over the base trust-based routing for detecting malicious nodes and providing security services through the established cryptographic mechanism. The proposed security-based algorithm is enough to accommodate and use latest cryptographic techniques in trust based routing for ensuring more participation through building confidence in the network. Opportunistic networks (OppNets) are a subclass of delay tolerant networks and are characterized by intermittent end-to-end connections. The scarcity in the network and the resource constraint of devices always restricts the use of cryptographic solutions for security needs in the OppNets for thwarting selfishness of the nodes. The simulation results are taken using ONE simulator and the results confirm that the application of security overlay above the base trust-based protocol helps in increasing the average performance by 35%. The study through complex networks analysis (CNA) provides a useful insight on the impact of human mobility toward routing Algorithm used Inter-Intra-Communication CNA (Complex network analysis) here routing are utility driven where ménages are forwarded to the nodes with higher utility. The security overlay design using SimBet as base routing protocol. This proposed protocol is trust based routing protocol. it uses the infrastructure nodes for surveillance and detecting malicious behavior. The cryptography solutions have been proposed for providing security services in the network is discussed in [9]. Using elliptic curve cryptography misbehavior detection 0f mobile node communicate with each other by using two ways one is the mobile nodes communicate directly if they are in radio range of each other, whereas others needs the aid of intermediate nodes to route their packets. Due to its primary characteristics, such as wireless medium, dynamic topology, distributed cooperation, MANETs is susceptible to different kinds of security attacks like worm hole, black hole, rushing attack etc. In this paper use of new methodology for intrusion-detection system named (EAACK) enhanced adaptive acknowledgement with elliptic curve algorithm (ECC). It is specially designed for MANETS. EAACK Demonstrates higher malicious behaviour detection rates in certain circumstance.ECC based digital signature can be used to provide cryptographic services like data integrity data, origin authentication and non repudiation protocol used (IDS) The results demonstrated constructive performance against watchdog, AACK and EAACK in case of receiver collision and limited transmission power false misbehaviour report and end to end delay is discussed in[10]. The Table II, shows the summary of various techniques used for secured data transmission.

3.CONCLUSION

In order to provide security for different types of attacks in the mobile ad hoc network. This paper presents the survey for detection and prevention of various attacks using improvised algorithms for MANET. Data privacy is a vital problem in MANET networks still there is a need for design and development of exclusive algorithms in MANETs.

Table -2: Summary of different techniques for secured data transmission.

Sl. No	Name of topic	Technique and mechanisms used	Simulator used	Description
1	Resisting black hole attacks on MANETs.	Self-Protocol Trustiness(SPT).Black hole Resisting Mechanism(BRM).	NS2	On both TCP and UDP traffic the mechanism succeeded in detecting black neighbors and enhancing the network performance for both. BRM-AODV is designed to mitigate the effect of black hole neighbors. The mechanism does not use cryptographic techniques which conserves the power and computation resources. BRM-AODV achieves an approximately constant PDR regardless the number of malicious nodes. BRM-APDV achieves a better PDR value than SAODV
2	Secure Transmission of packets Using D-S theory for Preventing MANET by Attacks.	Dempster Shafer theory	NS-2.35	Apply D-S theory for calculating the trust of nodes. Using this crypto approach prevent the network by passive attacks or by using trust value find out malicious behavior of nodes. The D-S is a mathematical theory of evidence and a theory of believable reasoning. D-S apply on the behavior of nodes so that it calculate the trust probability of nodes in network the range of probability from [0,1]. Probability values show the malicious or non-malicious nodes. This work packet delivery ratio gives better result as compare

				to existing work. Routing
3	Dynamic Forwarding Window Technique against DOS Attack in WSN	Profile based Protection Scheme(PPS) and Dynamic Forwarding window technique.	NS2(NS2.35)	In Forwarding window technique the attacker is detected in route request phase and prevention will be done in route reply phase. In proposed technique if any node floods the route request message more than the dynamic time then it will detect as attacker. The proposed work successfully detect and prevent DOS attack. The lessening of flooding tends to consume lesser amount of energy. Forwarding window concept has detected the malicious node and succeeded in reducing the damage caused to network by such malicious nodes.
4	Analysis of Detection Algorithm of sinkhole Attack and QOS on AODV for MANET	Individual Trust Managing	NS3	Individual trust managing technique to prevent against sinkhole attack. A detection technique is also analyzed for effective detection and removal of attacker node. Using AODV routing protocol a packet takes 0.3 milliseconds average time from source to destination. PDR in the presence of sink hole is 70% after introducing the detection technique PDR is increased up to 95% average.
5	Detection and Analysis of Jellyfish Attack in MANETs.	JFDV detection algorithm	NS2	The proposed algorithm analyzes packet delaying misbehavior of nodes and detect multiple JFDV attacker nodes.Once attacker node is detected, its address is saved in malicious list and re routing is initiated to prevent the attacker node from disturbing the performance of network. JFDV reduces average end-to-end delay and increases throughput by re-routing data packets through alternate route consisting non-malicious nodes. The proposed algorithm improves the network performance by increasing throughput and reduced end-to-end delay.
6	Detection of malicious node using Improved CONFIDANT Technique in Ad-hoc Networks	Improved CONFIDANT technique		Improved CONFIDANT technique resolves the significant problem of CONFIDANT technique such as detection and prevention of blackhole nodes, false reporting problem, network collision as well as providing QOS. This technique reduces the number of packet drop and provides security against malicious nodes. It also reduces false positive and false negative messages to spread in the network. It provide security against modification and fabrication of data packets by malicious node.
7	An Approach to detect Gray hole Attack son Mobile ad-hoc Networks	AODV with Intrusion Detection system(IDS)	OPENET,NETsim,NS3	This is capable of detecting the single & cooperative malicious gray hole nodes. Malicious node is isolated from the network by generating an alarm messages which can cause an extra overhead in network They provide a solution which can overcome the overhead of network caused by source node that send alarm message to all nodes about gray hole node. The proposed solution is try to improves network performance.
8	Hindrance and Riddance of Gray Hole Attack In MANETs Multipath Approach	Packet Update scheme and Gray hole detection algorithm	OPNET	The research concerned to provide solution to the gray hole attack by using multipath algorithm. Improved result after elimination of Gray hole attack in the simulation result. Elimination takes place on the network layer by broadcasting the information of the attacker node.
9	Cryptography-Based Misbehavior Detection and	Security based algorithm and use latest cryptographic technique	NS3, NS3	The main contribution of this work is the robust design of the security overlay, which provides adoptable security depending on the requirement of routing mechanism and backward linkage of malicious detection through trust depreciation. the

	Trust Control Mechanisms for Opportunistic Network system			cryptographic solutions have been proposed for providing security services in the network. The performance of this work depends upon the number of infrastructure nodes.
10	Improved MANET security usingElliptic Curve Cryptography and EAACK	EAACK with Elliptic Curve Algorithm	NS2,NS3	Intrusion detection scheme forms a fundamental constituent of internet safety. The result demonstrated constructive against watchdog, AACK, & EAACK. An effort to prevent the attackers from initiating a forged acknowledgement attacks. Lightweight Elliptic curve algorithm for digital signature in this proposed scheme.

REFERENCES:

[1].Mohamed A. Abdelshafy, Peter J. B. King "Resisting blackhole attacks on MANETs", IEEE, 2016, pp.1048-1053.

[2].Naveen Pathak, Anand Singh Bisen, Abhinav Vidwans "Secure transmission of packets using D-S theory for preventing MANET by attacks", IEEE (SCOPES), 2016, pp.2026-2030.

[3].Poonam Rolla, Manpreet kaur "Dynamic Forwarding Window Technique against DoS Attack in WSN", IEEE (ICMETE), 2016, pp.212-216.

[4].ShubLakshmiAgrwal, RakhiKhandelwal, Pankaj Sharma, SandeepKumarGupta"Analysis of detection algorith m of Sinkhole attack & QoS on AODV for MANET"IEEE (NGCT), 2016, pp.839-842.

[5].SakshiSachdeva,ParneetKaur"Detection and analysis of Je llyfish attack in MANETs", IEEE (ICICT), 2016, pp.1-5.

[6].Nirmala Devi, R.Sunitha "Detection of malicious node using improved CONFIDANT technique in Ad-hoc Network" IEEE (ICETECH), 2016, pp.604-610.

[7].Kusumalata Sachan, Manisha Lokhande "An approach to detect Gray hole attacks on Mobile ad-hoc Networks" IEEE (ICTBIG), 2016, pp.1-5.

[8].Jyoti Prabha Singh, Dinesh Goyal, Savita Shiwani, Vishal Gaur "Hindrance and riddance of Gray Hole attack in MANETs multipath approach", IEEE (ICCT), 2017, pp.1-5.

[9].Sanjay K. Dhurandher, Arun Kumar, Mohammad S. Obaidat "Cryptography Based Misbehavior Detection and Trust Control Mechanism for Opportunistic Network Systems", IEEE System Journal, 2017, pp.1-12.

[10].Pranjali Deepak Nikam, Vanita Raut "Improved MANET Security Using Elliptic Curve Cryptography and EAACK", IEEE (ICCN), 2015, pp.1125 – 1129.