RESEARCH ARTICLE OPEN ACCESS

Attacks Prevention and Detection Techniques In MANET: A Survey

Pranjali D. Nikam, Vanita Raut

Abstract—
Wireless sensor network is a set of distributed sensor nodes. Which are randomly deployed in geographical area to capture climatic changes like temperature, humidity and pressure. In Wireless Network MANET is a Mobile Ad-Hoc Networks which is a one self-configurable network. MANET is a collection of Wireless mobile node which is dynamically moves from one location to another location. Both attacks Active as well as Passive attacks is in MANET. It doesn't have a static structure. Security for wireless network is much difficult as compare to wired networks. In last few years many security and attacks issue are face many researchers in MANET. Attacks like Packet dropping attack, Black-Hole attack, Denial of Service attack, wormhole attacks and Packet modification attacks found in MANET. At the time of data communication all the above mentioned attacks access data easily without permission. To solve the problem of attacks in MANET and secure data communication use Intrusion Detection System. In This paper propose the survey of different kinds of attacks on MANET and Wireless sensor networks. This paper helps to young researcher for implement new hybrid algorithm for secure intrusion detection in MANET.

***Keywords*—** Mobile Ad-Hoc Networks, Wireless sensor networks, Intrusion detection system, Attacks. Ad-hoc On- Demand Distance vector, Network Security

I. Introduction

MANET is a collection of sensor nodes. Which are directly communicated with each other without any access point. MANET has not any fixed infrastructure. Nodes are communicated with each other using hop by hop or multi-hop mechanism in the network. Many types of techniques are developed by researchers in MANET for avoid the effect of malicious nodes on the network performance. Following three mechanisms are related to the protect network from malicious nodes. Watchdog – This mechanism implemented for improve the throughput at the presence of the of malicious nodes. Working of this mechanism is responsible for show the misbehavior of the sensor nodes in the MANET. TwoAck: - Watchdog mechanism has 6 weaknesses about the malicious node and network. TwoAck is never on the basis of Watchdog mechanism. Resason behind the implementation of TwoAck scheme is problem of collision receiver side and transmission power problem of the nodes. Links which have misbehave during the communication in the network. These kinds of links detect using TwoAck mechanism. AACK: - AACK mechanisms reduce the network overheads and keep the better performance for throughput in the network. [1]

There are two types of sinks present in communication network. One is static sink and mobile sink. In case of static sink information can be collected from source nodes statically. But mobile sink can be collect data from the whole network moving from one location to different direction. [16]

In wireless communication network is working with many routing protocols and MAC Protocols. AODV, DSDV and DSR are the three better routing protocols in wireless sensor networks. AODV Ad-hoc on demand distance vector routing protocol gives better result for parameters of networks. Packet delivery ratio, latency, energy consumption, throughput and packet drop ratio are the some quality of services of MANET. [17][18] Intrusion detection and prevention system is designed for stop the illegal access in the MANET. Some attackers attack on MANET to modify packets and break the links during communication. So intrusion detection system shows the attacks on attack and prevention system control as well as stop attacks on MANET. Packet drooping attack is a one kind of attack in MANET. [9][10] Malicious node is an only one reason of bad behavior of MANET. Malicious node decreases the performance of the network and Quality of Services of the network. Black hole attacks, Wormhole attacks, Routing attacks are the some kind of attacks in the MANET [11][12]

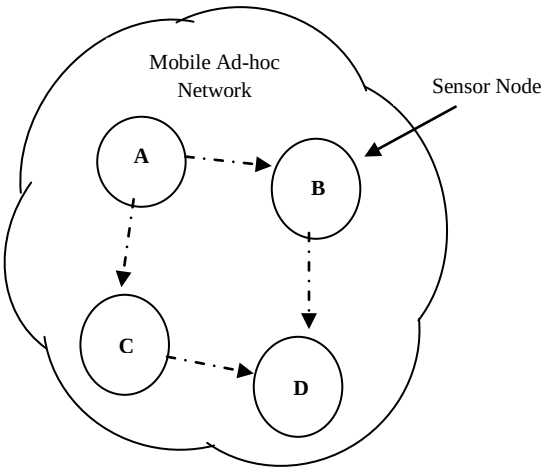

Figure 1. Structure of MANET

As shown in Figure 1 structure of MANET shows that the Node A sends packets through Node c and Node B to the node D. Node D is the Destination Node which is collect the data from node C and D. Using routing protocols network find out the shortest path for packet travels over the network.

II Literature Survey

In this paper author propose and Implement new IDS named Enhanced Adaptive Acknowledgement (EAACK).EAAK is developed for MANET. EAACK simulation shows the misbehavior of the malicious nodes and effect of malicious nodes on performance of the network. There are three techniques implemented in MANET for protect network from malicious nodes. 1) Watchdog 2) TwoAck 3) Adaptive Acknowledgement (AACK). MANET have a three possibilities of degrades performance wrong misbehavior, restricted transmission power and receiver side collision. All the above problems solve the using EAACK scheme. Problem of receiver side collision is a problem of intermediate node. When at a time two different nodes send the data to the single node. At that time collision will be occurs near the intermediate or receiver node. Problem of limited transmission power is arrives due to the less transmission range of the nodes. If one node can send packet to another node at same time if receiver nodes is not within the transmission range of the sender node, then sender is not able to send packet to the receiver node due to the less transmission range. In case of false misbehavior report problem arrives due to the wrong report send from one node to another node. TwoAck and AACK solve only 2 of 3 weaknesses. One weakness is Receiver collision and another is transmission power. But EAACK mechanism solves the false misbehavior attack problem which have not solved by TwoAck and AACK. Author used digital signature technique during the packet transmission process. EAACK is acknowledgement based Intrusion detection system. In this paper author implement or develop the RSA and DSA based digital signature mechanism in given proposed system. Author should be generates 1024 b RSA and DSA Key. Average Packet Delivery Ratio, Routing Overheads for EAACK is drastically better as compare to DSR, Watchdog, TwoAck and AACK. Technique. [1]

Author shows route discovery algorithm endairA implemented by authors is faulty. For hidden channel attack this algorithm is unsecure. Dynamic nature of MANET is a big reason behind the various kinds of attacks. At the time of route discovery hidden channel attacks attack on route. [2]On-demand location based unnamed MANET routing protocol (PRISM) developed by authors. This algorithm is achieves the security as well as privacy against the both insider as well as outsider antagonist. Author performs and analyze PRISM algorithm and compare it with existing algorithm. After performance analysis authors prove that the PRISM algorithm is more efficient and it's better for security as well as privacy preservation. Technique of tracking resistance implementation is the basic goal of authors. In this paper shows that the how to acquire the privacy in location based routing MANET's. Using PRISM technique authors achieves more privacy but never sacrifice security in MANET's. Better privacy as well as efficiency achieves by PRISM Protocol as compare to exiting Protocols results. Implementation of PRISM Protocol is on the basis of AODV Routing Protocol. It is also depend upon the one time public key mechanism as well as location based data. Route Request and Route Reply message is the working strategy of PRISM Protocol. Intermediate communications nodes are not shows the source and sink location. Intermediate nodes are not valid authenticated nodes at the time of route discovery between the sources to destination. Using one time security key source and destination is authenticated as well as encrypted. So PRISM Protocol is the better protocol for the privacy preservation in MANET as compare to other techniques. [3]

In wireless Communication different kinds of attacker attack on network. Active and Passive attacks are the two main kind of attacks categories in MANET and Wireless network. In case of Passive attack the attackers can be changed data or information without any kind of modification. But in case of Active attack attacker modify the packets during data communication. In MANET structure some malicious nodes modified packets and send to the source to destination. Information theoretic security based approach developed for the secure communication. This paper shows that the

performance of the network is better for the throughput under the misbehavior of malicious nodes. And average throughput is better under the active as well as passive attacks. [4] MANET is highly untrusted about security because of its unstatic or unconstant nature of the network. Many attacks are related to the routing attacks on routing protocols. Routing attacks always destruct and interrupt the MANET. But in network security many intrusion detection and intrusion prevention algorithms. Which is reduces the harmful as well as dangerous attacks on MANET. For the purpose of discover and reduces routing attacks on MANET authors propose the risk-aware response mechanism. Based on D-S evidence model risk aware approach is designed and developed. Authors compare the results of DRCIF with DRC and binary isolation. After analysis of graph authors shows the packet delivery ratio for the DRCIF is drastically better compare to other mechanisms. Delay and routing cost also less. DRCIF technique gives better result for PDR and Routing cost for varying node density from 10-50 nodes. [5]Routing attack is the major issue in MANET. This kind of attacks related to the routing path. Wormhole is also routing attack in MANET. Wormhole attacks are very harmful and break the routing link during the communication. Author proposed multilayered intrusion detection and prevention system for detect and stop the wormhole attacks on the MANET. MLDW layered framework include the estimator and calculators for node energy, packet drop calculation and estimation of the delay in the network. Basically wormhole attack belongs to AODV Route discovery mechanism. In the AODV route discovery phase only a wormhole attack effect on the MANET. When number of wormhole links are increased then the performance of the average throughput in the MANET can be changed. Average throughput for AODV through effected wormhole attack is better on MLDW framework. In case of varying the simulation time the average throughput again better. [6]

Sequence number attack is well known as black hole attack in MANET. Because in this kind of attack modified the sequence number at the time of communication. In this paper authors implemented the black hole attack detection method or approach to detect the attack in the network. Black hole attack detection method implemented using the AODV Routing protocol. In this paper author shows the simulation based black hole attack detection method. After simulation author prove that the when number of malicious nodes are increased from 1 to 5. Then packet delivery ratio for AODV routing protocol is better as compare to AODV under attack. PDR is very poor and decreasing order for AODV under attack. Again the in case of mobility speed varying from 10-70 m/s PDR for AODV is drastically better but performance of AODV under attack for PDR is very poor. Packet delivery ratio for AODV varying node density is drastically better as compare to AODV under attack and AODV under detection module. Average End to End delay for AODV varying mobility speed and node density is also better as compare to AODV under detection and AODV under attack module. [7] MANET in the presence of misbehaving malicious nodes degrades the network performance. Authors propose the novel idea for malicious nodes detection in AODV routing protocol. Protect the DOS attacks in routing protocols. In this paper author study and analyze the DOS attacks on the simulation basis using AODV routing protocol. Author proposed technique or method for gives the solution to identify malicious nodes in the MANET. In the authors implemented algorithm author set the on threshold point for number packet loss or drops in the network. Algorithm monitoring the sequence number for next hops and count the lost packets. If the numbers of dropped packets are greater than the threshold point set by the author. Then alert raised and detect the route of the nodes on the basis of dropped packets. Authors maintain here one log file for identify the nodes which are responsible for maximum packets drops. In this paper malicious node detection is on the sequence number. If any sequence number is in discontinuation then identify the malicious node. After simulation author proves that the malicious nodes are drop the number of packets. If number packets increased then it also affects on PDR, Routing load and throughput of the network. After malicious node detection and removal the performance of the network should be stable.[8] Intrusion detection system can be developed by authors for attack detection. To solve the problem of different kind of attacks on MANET. In this paper authors implement MAC Layer application to detect the malicious activities in the system. Many times attackers' attacks on sequence number and modify the sequence number in MANET. Application developed on MAC layer find out the attacks on sequence number. Authors developed Ad-hoc on-demand and multicast on-demand protocols for MANET. [9]

Authors proposed a new novel approach for detection of bad behavior during the routing in MANET. Due to the misbehaving of nodes, the function of information forwarding as well as routing can be affected. So authors propose one new model for bad behavior detection. Proposed technique working with very less routing overheads. Due to the minimum transmission of acknowledgement packets this model is drastically better compare to existing techniques. [10] To solve the problem of malicious nodes attacks on routing protocols. Performance improves of routing protocol with malicious nodes in MANET. Authors propose the trusted scheme for detection of malicious nodes. For observation of

behavior of nodes authors propose the new technique. Using trusted scheme for data transmission process uses only reliable as well as trusted path. In the result analysis authors compare the performance of trusted scheme with routing protocols and DSR. In case of packet delivery ratio when percentage of malicious nodes increases from 10 to 40%. Then packet delivery ratio for trusted scheme is better as compare to DSR and RP for 25, 50 and 100 node density. In case of average end to end delay also less compare to DSR and RP. [11] In case of AODV routing protocol attackers modify the sequence number as well as hop count. To prevent and detect this kind of attacks authors proposed technique. [12] Performances of MANET in case of flooding as well as black hole attack analyze by authors. After performance analysis packet delivery ratio for AODV protocol is very good as compare to RREQ AODV for varying pause time from 20 to 100 seconds. In case of node density the packet delivery ratio for AODV is better compare to other protocols. PDR with defense is drastically better when number of attackers increased from 2 to 10. But PDR without defense is very poor. [13]

Authors implement 2ACK techniques for routing scheme to reduce bad behavior in routing and reduce their effects. Idea behind the 2ACK scheme is to send the 2 hop acknowledgement packets in opposite direction of the routing path. In 2ACK technique only less received data packets are acknowledged to reduce extra routing overheads. Bad behaving sender as well as receiver affects on data packets. 2 ACK techniques is a network layer technique to detect the bad behavior link and reduce their effects. The 2 ACK techniques are implemented using DSR. 2 ACK Packet sends the opposite direction of data traffic route. Authors proposed 2 ACK technique is given better result compare to watchdog mechanism. In case of reliable data transmission, reliable route discovery, limited transmission power and limited overhearing range. [14] Most of the intrusion detection system of MANET's working with the watchdog mechanism. Authors propose the Adaptive Acknowledgment technique (AACK) for solving the problems of MANET's. AACK technique solves the problem of collision near the receiver side and limitation of the transmission power. Proposed technique gives drastically better performance compare to TWOACK and Watchdog mechanism. After result analysis results shows the performance of AACK mechanism is better for packet delivery ratio and routing overheads. The AACK technique is implemented using DSR Routing protocol. [15]The performance of AODV Routing [17] protocol is very good in case of achieving parameters of wireless sensor networks. Delay, energy consumption, throughput, routing and control overheads, packet drop ratio are the some quality o services of the wireless sensor networks. [18]

III Performance Review

Table 1. Working of Algorithms for different attack in MANET.

Paper No. In Reference	Technique	Use or Function of Algorithm
1	EAACK-IDS System	Shows Malicious Behavior detection rate
2	Route Discovery Algorithm-endairA	Hidden Channel Attacks
3	PRISM Protocol	Improve Privacy
4	Information Theoretic approach	To increase Throughput
5	Adaptive Time-wise isolation method	Identify Routing Attacks
6	MLDW Mechanism	Detect and Isolate Wormhole Attack
7	Black hole detection method	Improve Security on AODV
8	Malicious node detection Method	Protect against DOS Attacks
9	IDS Approach	Detection & isolate attacks
10	New reputation approach	Detection & Prevention packet dropping attacks
11	Trusted Scheme	Malicious Node Detection
15	2ACK	Routing Misbehavior Detection

Refer Table 1. For different kinds of attacks prevention and detection in MANET. This table helps to new researcher to implement new novel technique or hybrid technique.

IV Conclusion

The performance of the MANET and Wireless sensor networks should be degrades. Due to the loss of number of packets and misbehavior of the nodes during the communication. Malicious nodes modified packets and drop the packets during data transmission between source o destinations. It should be modify the packets and routing paths in network. Wormhole

attacks, Black hole attacks, Dos attacks directly effect on the networks performance. Always passive attacks attack on MANET. In this paper we have to do survey on the different kind of attacks on Routing Protocol in MANET. Here an author proves the MANET is insecure networks. Due to the it's dynamic nature. Some authors use the IDS System to intrusion detection and prevention in the network. So this paper is very good for design and implements a new hybrid protocol or algorithm for improve the security and prevent the malicious nodes. In future work, we have to design and implement new hybrid approach for malicious node and different kinds of attacks detection.

References

[1] E. M. Shakshuki, N. Kang, T. R. Sheltami, "EAACK - A Secure Intrusion-Detection System for MANETs", IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 60, NO. 3, PP-1089-1098, MARCH 2013.

[2] M. Burmester, B. Medeiros, "On the Security of Route Discovery in MANETs", IEEE TRANSACTIONS ON MOBILE COMPUTING, PP.1-9, 2008.

[3] K. El Defrawy, G. Tsudik, "Privacy-Preserving Location-Based On-Demand Routing in MANETs", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 29, NO. 10,PP.1-10, DECEMBER 2011.

[4] Y. Liang, H. V. Poor, L. Ying, "Secrecy Throughput of MANETs Under Passive and Active Attacks", IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 57, NO. 10, PP.6692-6701, OCTOBER 2011

[5] Z. Zhao, H. Hu, G. Ahn, R. Wu, "Risk-Aware Mitigation for MANET Routing Attacks", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 2,PP-250-260, MARCH/APRIL 2012

[6] Vandana C.P, Dr. A. F. Saviour Devaraj , "MLDW- A MultiLayered Detection mechanism for Wormhole attack in AODV based MANET" , IJSPTM, PP-29-41, Vol 2, No 3, June 2013

[7] V. Khandelwa, D. Goyal ," Black hole Attack and Detection Method for AODV Routing Protocol in MANETs", IJARCET, PP.1555-1559, Volume 2, Issue 4, April 2013.

[8] Kanchan, S. Rana, "Methodology for Detecting and Thwarting DoS in MANET" , IJCA Special Issue on "Network Security and Cryptography", PP.31-34,NSC, 2011

[9] T. P. Gondaliya, M. Singh, "Intrusion detection System for Attack Prevention in Mobile Ad-hoc Network", IJARCSSE, PP.638-641,Volume 3, Issue 4, April 2013.

[10] A. Sagar, A. Ukey, M. Chawla," Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET",IJSCI, PP.12-17, Vol. 7, Issue 4, No 1, July 2010

[11] Y. khamayseh, R. Al-Salah, M. Bani Yassein, "Malicious Nodes Detection in MANETs: Behavioral Analysis Approach", JOURNAL OF NETWORKS, VOL. 7, NO. 1,PP.116-125,JANUARY 2012

[12] R. H. Jhaveri, A. D. Patel, Jatin D. Parmar, Bhavin I. Shah, "MANET Routing Protocols and Wormhole Attack against AODVS" , IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.4,pp.12-18, April 2010.

[13] A.ANNAMALAI, V. YEGNANARAYANAN, "Secured System against DDoS Attack in Mobile Ad-hoc Network ", WSEAS TRANSACTIONS on COMMUNICATIONS, vol.11, issue.9, pp.331-341, 2012.

[14] Kejun Liu, Jing Deng, Pramod K. Varshney, Kashyap Balakrishnan, "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs" IEEE TRANSACTIONS ON MOBILE , vol. 6, no. 5, pp. 536-550, May 2007.

[15] A -Roubaiey, T. Sheltami, A. Mahmoud, E. Shakshuki, H. Mouftah, "AACK: Adaptive Acknowledgment Intrusion Detection for MANET with Node Detection Enhancement", IEEE International Conference on Advanced Information Networking and Applications, pp.634-640,2010.

[16] D. S. Waghole & V.S. Deshpande, \Reducing Delay Data Dissemination Using Mobile Sink in Wireless Sensor Networks." IJSCE-13, Vol-3, Issue-1, ISSN 2231-2307 pp.305-308, March-2013.

[17] D. S.Waghole & V. S. Deshpande , \Techniques of Data Collection with Mobile & static Sinks in Wireless Sensor Networks: A Survey," IJSER 13, Vol-4, Issue-10, ISSN 2229-5518, PP.501-505, Oct 2013.

[18] D. S. Waghole & V. S. Deshpande," Characterization of Wireless Sensor Networks forTrac &Delay," IEEE Conference, International Conference on Cloud & Ubiquitous Computing & Emerging Technology, pp 33-37, CUBE Nov-2013, Pune.