International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019

Efficient Intrusion Detection System to prevent the Packet Dropping nodes from Infrastructure Less Networks

Arshad Ahmad Khan Mohammad, Abbul Muqtadir, Anusha M

Abstract: ***Mobile ad hoc networks is wireless infrastructure free networks. It consist of heterogeneous mobile nodes. These nodes are distributed in wireless communication area. The characteristics of the network are adaptation, autonomous and self-formation and distributed peer to peer network. Applications of the network are military, health care and disaster recovery. Characteristics and applications of MANET demands reliable efficient communication. Multi hop communication is enable in the network by cooperation of the intermediate nodes. The intermediate nodes drop the packets due to either system fault or malicious behavior. Different way of packets drop due to system fault is recognized and isolated from malicious packet dropping nodes during the communication in existing "secure knowledge algorithm". However, it does not prevent the packet drop due to system fault in the network and it is very essential to enhance the performance and reliability of the communication. Thus the paper design "Efficient Intrusion Detection System to Avoid the Packet Dropping Nodes from Communication Route". Performance of the proposed IDS is tested in the simulator NS-2 and compare the results with existing work. Results are clearly indicating that the proposed IDS out perform in comparison with existing work in terms of reliability and packet delivery.***

Keywords: MANET, IDS, Packet dropping, routing, energy, and buffer.

I. INTRODUCTION

Mobile ad hoc network design aim is to enable internet connectivity everywhere all the time. Further the connectivity is enabled without the use of pre-defined infrastructure and allowing mobility to the nodes. The nodes are provided with the intelligence of the network so that they can act in as autonomous and self-forming way. The characteristics of MANET leads it to deploy in a critical & sensitive applications such as military, health care and disaster recovery. MANET is infrastructure free network, where nodes have freedom to mobile and deployment of nodes could happen in the arbitrary way. Communicating nodes could have more than one channel and deployed in standalone manner. The network is suitable for deploying in cost-effective and time effective environment [6,7].

Secure communication in MANET is challenging in MANET due to its multi hop peer to peer communication environment. Node communicate with other nodes directly within the radio range, otherwise nodes must rely on intermediate node for communication. Thus intermediate node must cooperate for communication [4].

Routing is the process of computing route between source to destination and forward the information in the computed routes. Majority of existing routing protocols computed route in the MANET based on the assumption that the nodes in the communication path are reputed and they follow the routing protocol specifications. Unfortunately the consideration of the existing routing protocols is false. The nodes fail to follow the routing protocol specification due to either malicious behavior or system fault. Thus the node drops the packets form routing path. The packet drop from communication path negatively effect on the performance of the network in terms of packet delivery, throughput and delay and congestion, lifetime [5].

The aim of the paper is to design the intrusion diction system to notice and stop the packet dropping nodes form communication path.

II. EXISTING WORK

Communication in any network is achieved by the construction of routing path between communicating nodes. The routing MANET is constructed by assumption that the nodes present in the communication path follow the routing protocol specification. Nodes could not follow the routing protocol specification due to either malicious behavior or system fault. The paper consider these nodes as packet dropping nodes. The packet dropping nodes are black hole node, cooperative black hole node, and false reporting node, and also node drops the packet due to insufficient energy and overflow of buffer [2,3].

Existing work "Secure knowledge algorithm" [1] identified the different way of packet dropping in MANET either by system fault and malicious behavior. Further the system prevented the malicious packet dropping nodes from communicating path only when the nodes do not drop the packet due to system fault.

Manuscript published on November 30, 2019.
* Correspondence Author

Arshad Ahmad Khan Mohammad*, Assistant Professor, Computer Science and Engineering, GITAM School of Technology, GITAM Deemed to be University, Hyderabad, India. Email: ibnepathan@gmail.com

Abdul Muqtadir, Lecturer , Mazoon College, Muscat, Sultanate of Oman, Email: mabdulmuqtadir@gmail.com

Anusha M, Associate Professor, Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Andhra Pradesh, India. Email:anushaaa9@gmail.com

The system fault packet drop considered in the existing work are energy, buffer and lifetime. However, the system only detect the system fault nodes in the communication path and did not prevent the.

Thus the paper aim is to design the effective intrusion detection system to prevent both malicious and system fault packet dropping nodes form communication path.

The proposed work prevent the packet dropping node due to malicious activities such as black hole node, gray hole node and system fault packet roping nodes such as packet drop due to energy and lack of buffer space

III. Proposed Work

The main aim of the proposed work is to prevent the malicious packet dropping node and packet drop nodes due to system fault form communication path. The proposed work achieve the goal by following contributions.

1. Preventing packet drop due to lack of energy
2. Preventing packet drop due to lack of buffer space
3. Preventing packet drop due to malicious behavior

A. *Preventing packet drop due to lack of energy*

In existing work finds the node which is dropping the packets then it check whether the drop of packet is due to lack of energy. If the packet drop is due to lack of energy then it does not consider the packet dropping node as the malicious node. However the system did not prevent the packet dropping nodes due lack of energy from communicating path. The packet drop due to constrained energy can exist in the MNAET several time due to the heterogeneous constrained resources of the nodes present in the network environment.

Thus the paper proposed the mechanism to prevent the packet drop due to the lack of energy nodes from communication path by computing packet handling capability of the node in its current energy. If node residual packet handling capability in not appropriate then the node is not allowed in the communication path. The residual packet handling capability with respect to energy of the node is computed by the following equation.

$$P_e = {}^{E_r}\!/_{\left(e_{tr} + e_{rx} + e_{pr}\right)} \dots \dots \dots \dots \dots \dots \dots (1)$$

Where,

P_e = Residual packet handling capability

with respect to energy of the node

E_r = *Residual energy of the node*

e_{tr} = *energy require to transmi the packet*

e_{rx} = *energy require to receive the packet*

e_{pr} = *energy require to process the packet*

B. *Preventing packet drop due to lack of buffer*

In existing work finds the node which is dropping the packets then it check whether the drop of packet is due to lack of buffer space. If the packet drop is due to lack of buffer space then it does not consider the packet dropping node as the malicious node. However the system did not prevent the packet dropping nodes due to lack of buffer space from communicating path. The packet drop due to constrained buffer space can exist in the MNAET several time due to the heterogeneous constrained resources of the nodes present in the network environment.

Thus the paper proposed the mechanism to prevent the packet drop due to the lack of buffer spacing nodes from communication path by computing packet handling capability of the node in its available buffer space. If node residual packet handling capability in not appropriate then the node is not allowed in the communication path. The residual packet handling capability with respect to buffer of the node is computed by the following equation [11, 12].

$$P_q = (1 - \alpha) * P_{qo} - (\alpha) * P_{qi} \dots\dots\dots\dots(2)$$

Where,

P_q = *Average Queue*

P_{qo} = *Average queue old*

P_{qi} = *Instant Queue*

If the queue size of the node is more than the average queue size then the node is not allowed to participate in the communication path.

C. *Preventing packets drop due to malicious behavior*

In order to prevent the malicious packet drop each node present in the network must listen to its neighboring node regarding packet operation by putting themselves in a promiscuous monitoring. The promiscuous mode is the network interface card setting in which each node can track its neighbor nodes packet operation such as number of packet received ad number of packets transmitted. The node maintain a table regarding the tracking information, which is shown in table 1. The table contains the information regarding how many number of neighbor nodes are present to the node and for each node how many packets are received and how many packets are transmitted. Table also compute the difference in the packet reception and transmission. If the difference is more than the certain predefined level than the node considered a malicious packet dropping node.

Consider a node source node-S" and destination node-D and malicious node-M and intermediate node "I", and it is shown in figure 1.

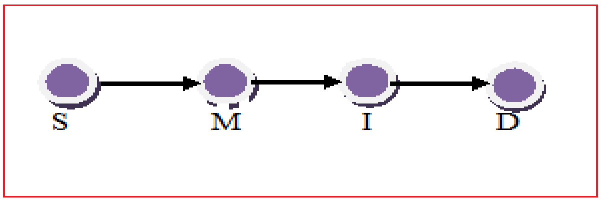

Figure 1 :- Communication Path in MANET with intermediate nodes

If the node detect the difference field in the table is more than the threshold packet dropping count than the node consider it as the malicious packet dropping node. Then node broadcast the information about malicious node to other nodes present in the network.

Table 1:- Promiscuous table of the node source node "S"

Neighbor nodes	Packet received	Packet forward	Difference
M			

IV. Performance Analysis

The performance of the proposed IDS is evaluated in the NS-2.35 [8,9,10] with necessary extension and compared with the existing "Secure knowledge Algorithm" in the identical environment. The performance metric considered are packet delivery, and throughput. The simulation environment composed of reputed nodes along with malicious and system fault packet dropping nodes. The parameters considered for the performance evaluation are shown in table 2.

Table 2 :- simulation-parameters

Simulation Parameters	Values
Nodes	10-100
Area (Network)	1000 * 1000
MAC	802.11
Radio Range	250 m
Time (Simulation)	1000s
Application	CBR
Size of packet	512 kb
Mobility	Random Way Point
Routing	Reactive

During simulation whenever node want to communicate with destination it computes the routing path reactively. The route computation for existing "secure knowledge algorithm" is based on the minimum hop count. Then the routing path composed of the malicious, system fault packet dropping nodes along with reputed nodes. The proposed algorithm computes the routing path which do not consist of the nodes which drops the packets due to either lack of buffer or lack of energy. The routing path in proposed approach composed of the malicious packet dropping nodes along with reputed nodes only, and there is no system fault packet dropping nodes present in the proposed approach routing path. Then source is intended to send the data to destination in terms of packets. The amount of packets acknowledged at destination and throughput and reliability of prosed and existing systems are shown in figures 2,3 and 4.

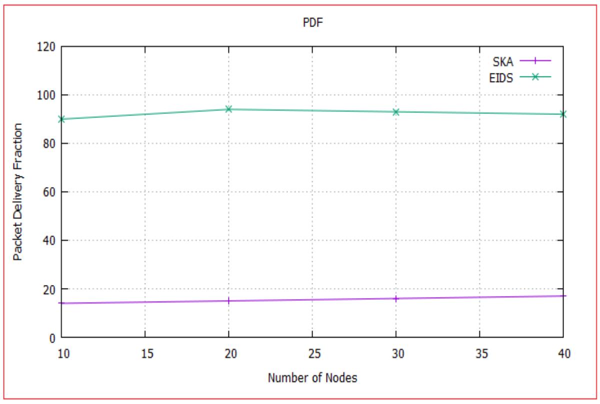

Figure 2 :- Packet delivery fraction comparison of SKA and EIDS

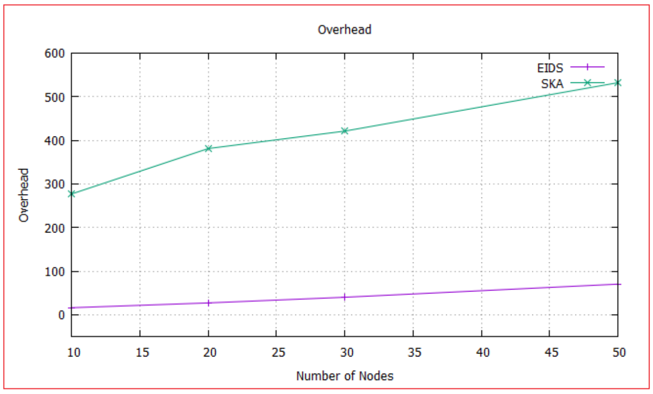

Figure 3 :- Overhead comparison of SKA and EIDS

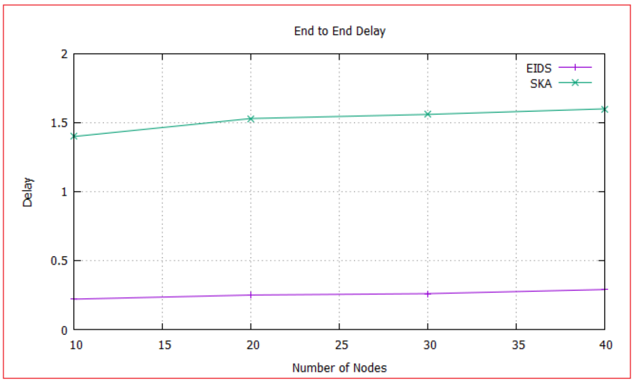

Figure 4 :- Delay comparison of SKA and EIDS

Results are clearly indicating that the proposed work overcome the packet drop due to system fault. Thus the packet delivery of the proposed work is comparatively high in comparison with "secure knowledge algorithm". The overhead of the existing protocol is high, as it check the reasons of the packet dropping by intermediate node after the packets are getting drop from the node. Throughput of the proposed work is high, as the end to end delay of the proposed work is low and it is due to the election of the non-congested intermediate nodes for routing path.

V. Conclusion

Characteristics of Mobile ad hoc networks leads it to deploy in sensitive and critical applications, where reliable communication is much desirable but it is challenging. Communication in MANET is enable by the cooperation of the intermediate node.

The node could not cooperate due to either malicious or system fault behavior. The paper proposed an efficient intrusion detection system to mitigate the both malicious and system fault behavior nodes from communication path. Performance results are indicating that the proposed IDS is more reliable in comparison with “Secure Knowledge Algorithm”.

REFERENCES

1. Siddiqua A, Sridevi K, Mohammed AA. Preventing black hole attacks in MANETs using secure knowledge algorithm. In2015 International Conference on Signal Processing and Communication Engineering Systems 2015 Jan 2 (pp. 421-425). IEEE.
2. Mohammad AA, Mirza A, Razzak MA. Reactive energy aware routing selection based on knapsack algorithm (RER-SK). InEmerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India CSI Volume 2 2015 (pp. 289-298). Springer, Cham.
3. Mohammad, Arshad Ahmad Khan, Ali Mirza, and Mohammed Abdul Razzak. "Reactive energy aware routing selection based on knapsack algorithm (RER-SK)." Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India CSI Volume 2. Springer, Cham, 2015.
4. Choudhary N, Tharani L. Preventing black hole attack in AODV using timer-based detection mechanism. In2015 International Conference on Signal Processing and Communication Engineering Systems 2015 Jan 2 (pp. 1-4). IEEE.
5. Mohammad AA, Mirza A, Vemuru S. Cluster based mutual authenticated key agreement based on chaotic maps for mobile ad hoc networks. Indian Journal of Science and Technology. 2016 Jul;9:26.
6. Kurkowski S, Camp T, Colagrosso M. MANET simulation studies: the incredibles. ACM SIGMOBILE Mobile Computing and Communications Review. 2005 Oct 1;9(4):50-61.
7. Elderfield J, Manet E. Manet and the Execution of Maximilian. The Museum of Modern Art; 2006.
8. Issariyakul T, Hossain E. Introduction to network simulator 2 (NS2). InIntroduction to network simulator NS2 2009 (pp. 1-18). Springer, Boston, MA.
9. Ros FJ, Ruiz PM. Implementing a new manet unicast routing protocol in ns2. Dept. of Information and Communications Engineering University of Murcia. 2004 Dec.
10. Nayak AK, Rai SC, Mall R. Computer Network simulation using NS2. CRC Press; 2016 Aug 19.
11. Mohammad, Arshad Ahmad Khan, Ali Mirza Mahmood, and Srikanth Vemuru. "Energy-Aware Reliable Routing by Considering Current Residual Condition of Nodes in MANETs." Soft Computing in Data Analytics. Springer, Singapore, 2019. 441-452.
12. Lin, Dong, and Robert Morris. "Dynamics of random early detection." ACM SIGCOMM computer communication review. Vol. 27. No. 4. ACM, 1997.