A Reliable Research to Preserve Security in Infrastructure less Networks: MANET

M. Grace Prasana, S.Ancy, K.Cornelius

Abstract— ***Mobile ad hoc networks (MANETs) are a unique wireless network which does not relay on any defined infrastructure. Compared to wired networks, MANETs can be attacked easily due to absentness of centralized monitoring authority. The nodes in these networks are dynamic and they set the path to transfer data. Due to this nature of MANET there is a need to incorporate routing protocol with security mechanism. The available cryptographic algorithms supports authentication to escape from passive and active attacks. Here this problem is addressed using Intrusion detection mechanism (IDM) and Position-based Opportunistic Routing protocol (PORP) in a reliable and timely manner.***

Keywords: MANETs, IDM, PORP,CP-ABE

I. INTRODUCTION

Mobile adhoc networks represents a group of self-configured free flow structure less mobile nodes. Security is vital pre-requisite of MANETs.To ensure reliability there is a need to check confidentiality, availability, authentication and integrity among the mobile nodes. MANETs are prone to various attacks.

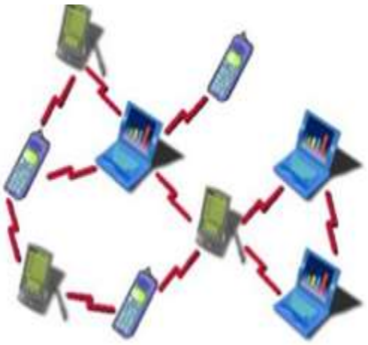

Fig: 1.MANET Layout

The passive attack causes confidentiality threat. Eavesdropping is a type of attack were confidentially is lost. A black-hole is a node that communicates to the source node that it is the nearest node to destination node and results in security problem. Thus the source sends the data to malicious node and the data may get lost. One type of attack called wormhole attack, where the attacker gets the data packet from one position and transfers to far away distance. This problem can be irradiated through available geographic routing to forward data packets through hop-by-hop fashion. The major drawback of this is location inaccuracy. And another method is digital signature used to address this type of attack. Geographic routing is a prominent method of routing when the nodes are highly dynamic in nature. There is a chance of node failure if the nodes are not in specific range. Intrusion is any action that prevents integrity, confidentiality or availabity of resources in MANET. Intrusion detection mechanism (IDM) is a widely used mechanism for identifying intrusion.

II. LITERATURE REVIEW

Kaushal.S and Aggarwal,R [1] This paper analyzes the performance measure of MANET infrastructure using AODV protocol. Here the wormhole attack is addressed and the malicious node identification is done.

Farhan Abdel-Fattah, Farhan Abdel-Fattah, Khalid A. Farhan, Feras H. Al-Tarawneh, Feras H. Al-Tarawneh[2] The survey focus on various attaks on MANET structure and depicts the various vulnerable attacks. Arathy, K. and Sminesh, C,[3] pointed out a strategy to detect single and collaborative black hole attack with minimum overhead. This algorithm addressed the additional route request.Martin Appiah [4] author identified the impact of dynamic MANET structure.RWP and MDL were the two models used for verification.

S. Doss et al.,[5] this work proposed a technique for prevention and detection of jelly fish attack. This mechanism combines authenticated routing-based framework for detecting attacks.Houssaini, M.A.; Aaroud, A.; El Hore, A.; Ben-Othman, J [7] the analysis was based on special kind of service attack called DOS. The signal can be jammed which leads to loss of message. The approach used for detecting intrusion by applying statistical process control.SPC is the key element of the detection of jamming attack.

X. Liu, Z. Li, P. Yang, and Y. Dong[8]this paper describes a methodology for finding the path and categorize the routing into effective and reliable manner. The purpose of this work is to enhance the references and knowledge about content routing.

D. Ahmed and O. Khalifa [9], the authors explained a detailed study on MANET applications, challenges and issues.

G. M. Borkar and A. R. Mahajan, [10] In this paper, the standard ad hoc multi-path distance vector protocol is used to establish the routing in adhoc network.

Y. Wang, I.-R. Chen, J.-H. Cho, A. Swami, and K. S. Chan,[11] This paper illustrates the multidimensional trust based algorithm. In addition the simulation results shows trust-based algorithm against a non-trust-based algorithm performance. This method ignores out malicious nodes

Revised Manuscript Received on 14 September, 2019.

M. Grace Prasana, Assistant Professor, Department of Computer Science & Engineering, St.Peter's Institute of Higher Education and Research, Chennai, Tamilnadu, India. (Email: gr_prasana@yahoo.com)

S.Ancy, Assistant Professor, Department of Information Technology, Jeppiaar Institute of Technology, Tamilnadu, India. (Email: sancyit@gmail.com)

K.Cornelius, Assistant Professor, Department of Computer Science & Engineering, St.Peter's Institute of Higher Education and Research, Chennai, Tamilnadu, India. (Email: cornelius851@gmail.com)

which produces various attack in the network.

A. Mehmood, A. Khanan, A. H. H. Mohamed, S. Mahfooz[12] this paper indentifiesand illustrates the routingconcept by employing awareness of the current traffic flow and other factors such as speed difference, direction, connectivity level and node distance from its neighbours by using the intelligent technique.

F. A. Khan, M. Imran, H. Abbas, and M. H. Durad [13] ,this paper uses special nodes called DPS nodes, the work of these nodes is to repeatedly monitor the activity of other nodes attached in a network. When a DPS node identifies a node with faulty behaviour, it declares that suspicious node as a wormhole node by sending message to remaining nodes in the network. The message from the faulty node is ignored and it is discarded.

P. Vijayakumar, V. Chang, L. J. Deborah, and B.S. R. Kshatriya[14] The authors stated the need for secure key management and distribution in various fields which enables secure transmission of data in groups.

III. SYSTEM MODEL

Intrusion detection mechanism (IDM) consists of four parts namely data aggregation, Fault detection, Intrusion models and Response to Intrusion.

1) Data aggregation: Gathering and processing data. Tasks such as transferring and storage of data's are performed.

2) Fault Detection: Obtained packets are verified for intrusions. Verified data is sent as the response.

3) Intrusion Model: An expert system has the knowledge of identifying intrusion.

4) Reply to Intrusion: When the information is received this component will predict the chance of intrusion and how to manage.

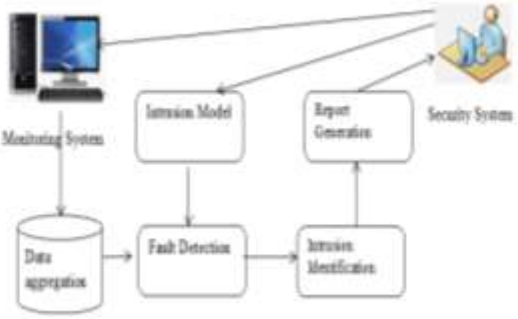

Fig 2 View of Intrusion detection system

A. *Position based opportunistic Routing (POR) works as follows:*

1) The location of nodes to be determined along with its neighbour information.

2) The node A transmits a packet to node G, where A calculates the forwarder list based on distance and destination and incorporates the information list in the header. The nearer node will have the priority.

3) The list of nodes near the transmitter node will receive the packet. All the receiving node will checks for its position and will wait for n time slots. And then discard the packet if it is not in highest priority.

4) This pattern is followed till the packet reaches the sink.

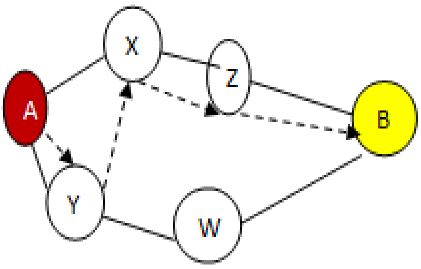

Fig 3 Possible POR Path.

In figure 3 source node A tries to transfers a packet to destination B. Using POR routing the nearest neighbouring node is selected by it position and it is indicated by dotted arrows.

The robust nature of POR routing provides scalability. The location information limits broadcasting range. In turn the reply is obtained from the receiver. This mechanism is completely based on the knowledge of forwarding node.

IP Header	Seq_No	My_X	My_Y

Beacon Packet Structure

IP Header	Seq_No	My_X	My_Y	Dst_X	Dst_Y

	hops	Forwareder_No	Forwareder_list		

Neighbor1(ip)	Neighbor2(ip)	………….

Fig 4 Packet structure

B. *Information Management*

In the general network every node maintains a list of its neighbouring node. The list is updated by one hop. The previous hop piggybacked in packet header. Once the packet is transmitted in multicast pattern every node has its own track to predict duplication. The forwarding table is generated at start point of packet transmission. The can be generated in less time. As soon as a node receives data for transmission, the transmitter has to wait for certain duration since the data to be placed into the forwarding list. If there exist no forwarder, then the packet will be placed in waitlist till it obtains the forwarding.

If a dead-end appears, due to its dynamic nature this can be solved with in a short span. The simulation results shows the mobility nodes with selecting nodes neighbour based on its position.

C. *Feedback Mechanism*

Usually the sender gets an acknowledgement after the message is received by the destination. Here the proposed mechanism which suggests, on receiving each packet every node sends an acknowledgement message to its own sender. By comparing the ACK from destination node and neighbouring node we can identify the packet drop.

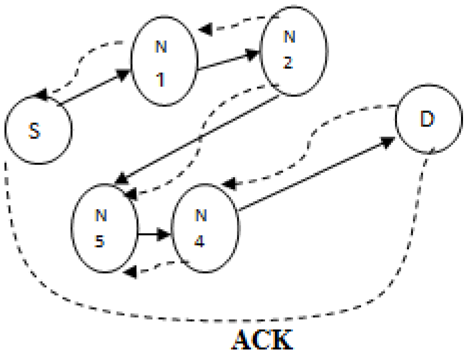

Fig 5 Feedback Mechanism

In Fig 5 solid arrow shows the packet transmission path and dotted arrow shows the acknowledgements among intermediate nodes as well as ACK between source to destination

D. CP-ABE

Cipher text-Policy Attribute based encryption the attributes of secret key is placed functionally into the key after while encryption. Then the data packet is sent to its destination. If the policy is well placed the destination node can decrypt the data packet. The intermediate node cannot decrypt

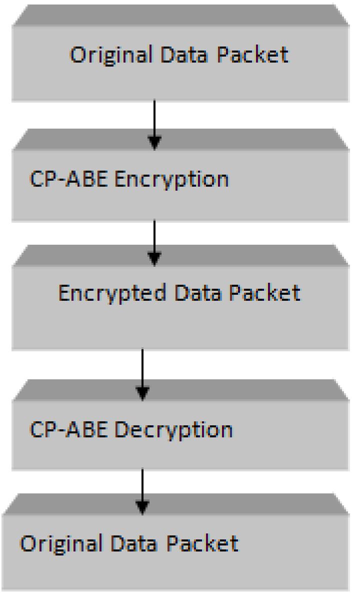

Fig 6 Encryption and decryption CP-ABE

IV. EXPERIMENTAL RESULTS AND DISCUSSION

The dynamic nature of nodes in MANET where the source node tries to transmit the message to destination based on position of neighbour nodes. Identifying the neighbour nodes is shown the figure 5.

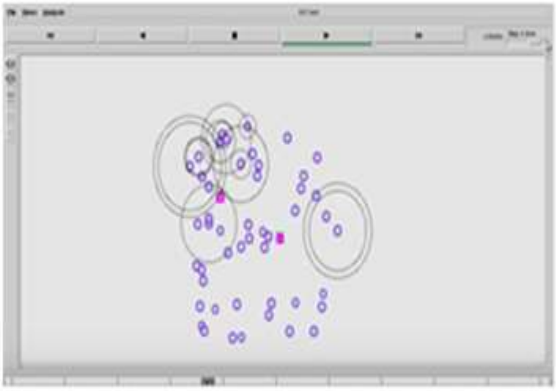

Fig 7 Communication between nodes and neighbour node selection

The packet loss when compared to other routing protocols.

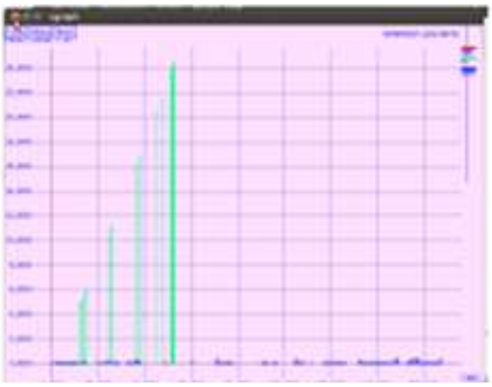

Fig 8 Packet Loss Ratio

The delay ratio of nodes when waiting to transmit data packets to neighbouring nodes.

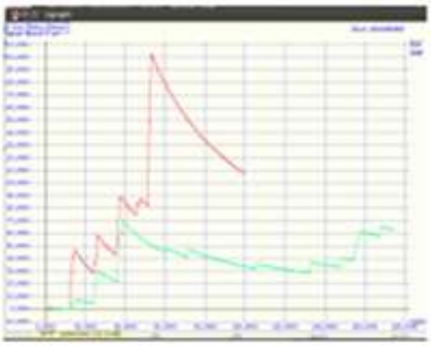

Fig 9 Delay ratio of position based Routing

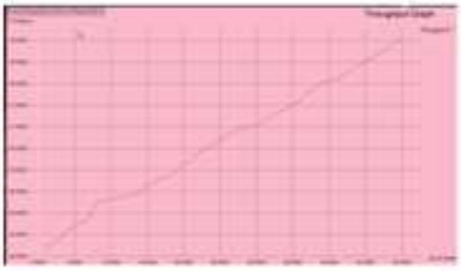

Fig 10 Throughput ratio

V. CONCLUSION

In this paper intrusion detection mechanism is used is monitor the malicious node in the decentralized network. The position based routing shown as a reliable mechanism of transferring data packet source to sink. However other than this CP-ABE is proposed for decentralized network for efficient and secure data retrieval.

REFERENCES

1. Kaushal, S., and Aggarwal, R. A study of Different types of attacks in MANET and performance analysis of AODV protocol against Wormhole attack. IJARCET (2015), 301-305.
2. Farhan Abdel-Fattah, Farhan Abdel-Fattah, Khalid A. Farhan, Feras H. Al-Tarawneh, Feras H. Al-Tarawneh Security Challenges and Attacks in Dynamic Mobile Ad HocNetworks MANETs 2019 IEEE Jordan International Conference on Electrical Engineering and Information Technology(JEEIT)
3. Arathy, K. and Sminesh, C., “A Novel Approach for Monitoring of Single and Collective Black Hole Attacks in MANET”, in Elsevier,Recent Advancements and Effectual Researches in Engineering,Science and Technology – RAEREST Vol. 25, pp. 264–271, 2016.
4. Martin Appiah “The impact of mobility models on theperformance of mobile ad hoc network (MANET)” 2016 International Conference on Advances in Computing and Communication Engineering (ICACCE).
5. S. Doss et al., "APD-JFAD: Accurate Prevention and Detection ofJelly Fish Attack in MANET," in IEEE Access, vol. 6, pp. 56954-56965, 2018.
6. Geetha.K ,N.Sreenath, “Mitigation of session hijacking in mobile adhoc networks”, International Journal of Applied Engineering Research, Volume 10, pp. 34281-34287, 2015.
7. El Houssaini, M.A. Aaroud, A. El Hore, A.; Ben-Othman, J.Detection of Jamming Attacks in Mobile Ad Hoc Networks UsingStatistical Process Control. Procedia Comput. Sci. 2016, 83, 26–33.
8. X. Liu, Z. Li, P. Yang, and Y. Dong, ‘‘Information-centric mobile ad hoc networks and content routing: A survey,’’ Ad Hoc Netw., vol. 58, pp. 255–268, Apr. 2017.
9. D. Ahmed and O. Khalifa, ‘‘An overview of MANETs: Applications, characteristics, challenges and recent issues,’’ Int. J. Eng. Adv. Technol., vol. 6, no. 4, p. 128, Apr. 2017.
10. G. M. Borkar and A. R. Mahajan, ‘‘A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks,’’ Wireless Netw., vol. 23, no. 8, pp. 2455–2472, 2017.
11. Y. Wang, I.-R.Chen, J.-H. Cho, A. Swami, and K. S. Chan, ‘‘Trust-based service composition and binding with multiple objective optimization in service-oriented mobile ad hoc networks,’’ IEEE Trans. Services Comput., vol. 10, no. 4, pp. 660–672, Jul./Aug. 2017.
12. A. Mehmood, A. Khanan, A. H. H. Mohamed, S. Mahfooz, H. Song, and S. Abdullah, ‘‘ANTSC: An intelligent Naïve Bayesian probabilistic estimation practice for traffic flow to form stable clustering in VANET,’’ IEEE Access, vol. 6, pp. 4452–4461, 2018.
13. F. A. Khan, M. Imran, H. Abbas, and M. H. Durad, ‘‘A detection and prevention system against collaborative attacks in mobile ad hoc networks,’’ Future Gener. Comput. Syst., vol. 68, pp. 416–427, Mar. 2017.
14. P. Vijayakumar, V. Chang, L. J. Deborah, and B. S. R. Kshatriya, ‘‘Key management and key distribution for secure group communication in mobile and cloud network,’’ Future Gener. Comput. Syst., vol. 84, pp. 123–125, Jul. 2018.
15. Shengbo Yang, Feng Zhong, Chai Kiat Yeo, Bu Sung Lee, Jeff Boleng Position based Opportunistic Routing for Robust Data Delivery in MANETs GLOBECOM 2009-2009 IEEE Global Telecommunications Conference.