Contemplate on Intrusion Detection & Prevention System (IDPS) in MANET

SHARMASTH VALI Y[1], SHAKKEERA L[2]

[1, 2] *Assistant Professor, Department of CSE, Presidency University, Karnataka, India.*

Abstract— Recently, the extensive availability of wireless communications has led to the growth and importance of wireless mobile ad hoc networks (MANET). Wireless mobile ad hoc networks have recently increased in size and significance due to the widespread availability of wireless communications (MANET). As a result, malicious nodes can blend in with the rough channel conditions and decrease the detection precision of traditional secure routing algorithms. In such cases, monitoring the packet loss rate is insufficient to precisely pinpoint the reason for a packet loss. Malicious nodes which work in the background of different harsh channel conditions tend to reduce accuracy, packet loss rate to identify is thread. So it proposes to differentiate and eradicate the packet loss and reduction in overall detection accuracy survey by viewing in different harsh channel conditions. Role played by IDS and other different layers by applying its feature to harsh channel conditions. The system is going to measure indirect trust of the nodes and should target the malicious nodes if it is predicted and should take necessary action. Lastly, it gives an overview of the functioning and reaction of the different approaches.

Indexed Terms— MANET, IDS, IPS, packet dropping.

I. INTRODUCTION

MANET (Mobile ad hoc network) is a multi-hop wireless network which is composed of non-centralized administration. Nodes are going to play the role of router and compel the nodes to cooperate for the network. Resources are consumed very rapidly, so that the node activities can take place. The main advantage in MANET over the network is a fixed topology including scalability, flexibility and low-cost administration i.e without infrastructure. The disadvantage is finding an accurate model that represents human mobility whilst remaining mathematical traceable remains an open problem due to the large range of factors which influence it. In MANET [16][17], many harsh channel conditions like link error due to mobility, which is causing packet dropping in the network. Also, to have the network knowledge of malicious nodes, where it can camouflage its behavior under the conditions of packet dropping or due to link failure. Packet loss due to malicious node or link failure becomes a challenging problem.

The problems with watch dogs, such as receiver collisions and low transmission power, have been resolved by the TWOACK method. TWOACK will use the ACK it receives to identify the problematic links. Each data packet that travels over every third consecutive node along the routing path thus receives an ACK. [2]. The node that is two hops away from each node receives an ACK from that node. The TWOACK system also addresses receiver collision and restricted sent power. However, when receiving an ACK from a node two hops away from the sender, the network overhead rises. TWOACK has significant overhead and high energy usage.

The main issue in the network is packet dropping, once the packet dropping is happening in the network, it is going to slow down the network activities. Consumption of energy is very high in the environment, also an important concern. This type of environment is very much susceptible to different types of attacks [20]. So, reactive routing protocols are more vulnerable to a variety of routing attacks in this environment, where nodes are cooperative. Routing algorithms are very much cooperative for a variety of attacks. Attacks in the routing algorithm are sleep deprivation, packet dropping, black hole attack, rushing attack and sybil attack. Here the routing protocol deals with node mobility, battery consumption and bandwidth.

Intrusion Detection Systems (IDS) [1][10] which is going to monitor and detect suspicious activities when trends happen and action has to be taken. Intrusion Prevention Systems (IPS) comes into action before any suspicious activities take place. When any suspicious activity is alerted, the system springs to take action like blocking the activity from continuing, strengthening the firewall to prevent the changes. IDS is going to notify any type of attack and it has to generate the alert and it has to take appropriate action and on other hand IPS will come into action before any type of attack happens. So, IDS and IPS are network level defense mechanisms. The main difference is to provide protection to the network environment with respect to detection and prevention systems.

Some of the myths about IDS/IPs are:

1. IDS/ IPS are two separate solutions.
2. IDS need to detect the malicious behavior, whereas IPS come into action before regular activities take place.
3. IDS gives many false positive rates and it eventually replaces the firewall.
4. There are very few security admins required if you deploy an IDS.

II. RELATED WORK

Several works have been done on MANET [10] for detection and prevention systems where they can prevent and detect suspicious activity from packet dropping and data integrity. So, intrusion detection [12][13] has been categorized into reactive and proactive mechanisms. Also, intrusion prevention systems deploy into the reactive category. SHEATH [4] proposes to secure routing against dropping and data integrity. SHEATH system proposes self and mutual key reliant prevention and appearance frequency-based behavior certainty measurement on routing paths [9]. So, the self key prevention scheme exploits the encrypted value of the sequence number as a normal pattern and determines its route reply in result. Mutual key in data forwarding between the communicating nodes has to prevent the data integrity attack.

AIDST [5][18] system is to discern and eradicate the intruders from the network. They have incorporated multi-dimensional trust [3] parameters with subjective logic theory, so that it is effectively going to detect and to confirm the attack behavior [19]. Also, it has been proposed to measure indirect trust [7] of a node using subjective logic theory for effective results. They have attained high performance in terms of detection accuracy, overhead and energy consumption with existing AIPD AODV.

CID [6] this paper proposes to accurately discern and eradicate the intruders from the detection engine after continuously monitoring their activities. They have segregated their IDS system in local and IDs systems. In local detection they have to monitor the network activities and differentiate the packet loss happened due to harsh channel conditions from using the features of physical layer, MAC land Network layer. Depending on the results of local detection engine, IDS proposes DS theory to take evidence from the neighbor nodes i.e is the direct trust in confirming the malicious node.

III. OVERVIEW OF PROPOSED METHODOLOGY AND SYSTEM MODEL

The below system model is segregated into four sections: monitoring of data, observing lower layer impact, IDS & IPS, trust estimation which will provide a secure routing. In data observing phase in routing layer, where data collection process takes place, so that it can make comparison with the current date. We have made clear observations that packet loss happened intentional or unintentional, which is a challenging problem.

For example, node X wants to send packets to node Y, at the initial stage. So, node X forwards RTS messages to node Y and it is going to wait until the medium is free.

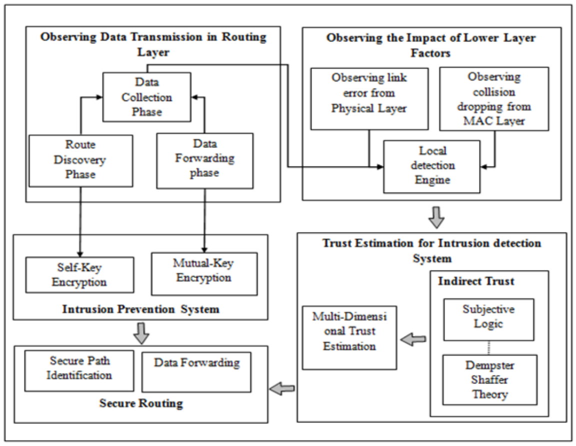
Observing Data Transmission in Routing Layer
Data Collection Phase
Route Discovery Phase
Data Forwarding phase
Observing the Impact of Lower Layer Factors
Observing link error from Physical Layer
Observing collision dropping from MAC Layer
Local detection Engine
Self-Key Encryption
Mutual-Key Encryption
Intrusion Prevention System
Trust Estimation for Intrusion detection System
Indirect Trust
Subjective Logic
Dempster Shaffer Theory
Multi-Dimensi onal Trust Estimation
Secure Path Identification
Data Forwarding
Secure Routing

Fig. 1 - overall view of IDPS

So RTS message may suffer probability, collision can be occured due to another node can forward the RTS message to Y at the same time. Y replies to X with a CTS message, on receiving an RTS message successfully from X.Otherwise CTS may suffer the probability. So, it takes some unique features to differentiate the packet loss due to mobility and congestion from the malicious actions.

The primary goal in link error is due to reduction in false positive rate. At the same time of data collection, observing what type of harsh channel conditions are there to prevent the failure of findling malicious nodes will become a challenging problem. So, once the job observing data is done then it will proceed to take the trust estimation of each and everyone the same as the routing table. MAin focus is to find packet dropping happening due to mobility, network congestion and link error or failure. After which it passes through trust estimation. How we are going to find the trust of the node. Packet loss in MAC layer due to network condition is considered.

To estimate the trust level in both ways i.e direct and indirect trust, which is determined by few trustworthy evidence for overall evaluation. For example the nodes A and B are neighbors and the local detection engine of node A and B identifies that the node B is suspected. If a node B fails to generate an intrusion alert to prove that a node B is a suspected node, the node A generates an alert for node B after waiting for t time. Node C, D, E are the neighboring nodes of node A and B. Node E and C claims about node S is a suspected one, but node D claims the node S as a legitimate node. So, when the role of IPS comes, self key is used in route discovery process and mutual key is used in data forwarding process. Data privacy is not the goal of self and mutual key. The main objective is to identify malicious nodes and take necessary action once it is detected. Once the malicious node is detected then it is the duty of IDS to take necessary action like to eradicate the node or make an alert to neighbor nodes.

CONCLUSION

In this proposed work the objective of packet drop is to identify and reduce energy consumption when it comes for multidimensional layers. The truthful packet loss is differentiated in terms of some harsh channel conditions. This process is going to improve the detection accuracy when a trust estimation is applied. IDS/ IPS play vital roles which are essential to integrate the mobility of nodes to secure the routing path.Further work will be on implementation of the work in Network Simulation 2 (NS2) for comparative analysis for classifying IDS/ IPS. Lastly, inthe next continuation work on implementation will achieve better simulation results on detecting packet fall attacks with high sensing accuracy and significant energy consumptions.

REFERENCES

[1] Sharmasth Vali Y, Prakash N, Shakkeera L, "An Efficient and Lightweight Intrusion Detection System for Mobile Ad Hoc Networks" in Lecture Note in Mechanical Engineering (LNME), Springer Nature Singapore Pte Ltd. 2022.

[2] Sharmasth Vali Y, Prakash N, Shakkeera L "An Efficient Diagnosing Anomalies and Discovering Secure Route Path in MANET DADSR" in the International Journal of Analytical and Experimental Modal Analysis, Vol. 12, Issue 9, September 2020.

[3] Muthumari L and Sharmasth Vali.Y "Trust based malicious node detection & certificate revocation based on cluster head for MANET" in International Journal of Pure and Applied Mathematics, Vol. 119, No. 15, pp. 385-390, 2018.

[4] Sharmasth Vali.Y, Prakash Natarajan, T.R. Rangaswamy "Proactive Hybrid Intrusion Prevention System for Mobile Ad-hoc Network" in Journal of Intelligent Engineering & Systems, ISSN No.2185-3118, Vol. 10, No.6, December 2017.

[5] Sharmasth Vali.Y, Tiruchirai Rangaswamy "An Anomaly-Based Intrusion Detection System with Multi-Dimensional Trust Parameters for Mobile Ad-hocNetwork" in Journal of Intelligent

Engineering & Systems, ISSN No.2158-3118, Vol. 10, No.4, August 2017.

[6] Y. Sharmasth Vali, T.R. Rangaswamy "An Efficient Cross-Layer based Intrusion Detection System for Mobile Ad-hoc Networks" in Journal of Theoretical and Applied Information Technology, ISSN No.1992- 8654, Vol. 95, No.1, 2017.

[7] Sharmasth Vali Y "Trust based malicious node detection & certificate revocation based on cluster head for MANET" in International Conference on Advanced Scientific Innovation in Science, Engineering and Technology(ICASISET – 2018) at Bharath Institute of Higher Education and Research, Chennai during 11 th to 13 th April 2018.

[8] Shakshuki, Elhadi M., Nan Kang, and Tarek R. Sheltami, "EAACK—A Secure IntrusionDetection System for MANETs", IEEE Transactions, Vol.60, No.3, pp.1089-1098, 2013.

[9] Sharmasth Vali Y, Prakash N, Shakkeera L "An Efficient Diagnosing Anomalies and Discovering Secure Route Path in MANET DADSR" in the International Journal of Analytical and Experimental Modal Analysis, Vol. 12, Issue 9, September 2020.

[10] De Morais Cordeiro, Carlos, and Dharma P. Agrawal "Mobile ad hoc networking", Center for Distributed and Mobile Computing, pp.1- 63, 2002.

[11] Zhang, Yongguang, Wenke Lee, and Yi-An Huang, "Intrusion detection techniques for mobile wireless networks", Wireless Networks, Vol. 9, No.5, pp. 545-556, 2003.

[12] Chen, Thomas M., and VaradharajanVenkataramanan, "DempsterShafer theory for intrusion detection in ad hoc networks", IEEE Internet Computing, Vol.9, No.6, pp.35-41, 2005.

[13] Fung, Carol, "Collaborative intrusion detection networks and insider attacks", Ubiquitous Computing, and Dependable Applications, Vol.2, No.1, pp.63-74, 2011.

[14] Fung, Carol J., et al, "Dirichlet-based trust management for effective collaborative intrusion detection networks", IEEE Transactions Network and Service Management, Vol.8, No.2, pp.79-91, 2011.

[15] I. Chlamtac, M. Conti, and J.J-N. Liu "Mobile ad hoc networking: imperatives and challenges", Ad hoc Networks, ELSEVIER, Vol.1, No.1, pp.13-64, 2003.

[16] C.M. Cordeiro and D.P. Agrawal "Mobile ad hoc networking", Centre for Distributed and Mobile Computing, pp.1-63, 2002.

[17] Y. Zhang, W. Lee, and Y. Huang, "Intrusion detection techniques for mobile wireless networks", Mobile Networks and Applications, Vol. 9, No.5, pp. 545-556, 2003.

[18] B. Venkat, V. Vijay, and T. Uday, "Subjective Logic Based Trust Model for Mobile Ad hoc Networks", In: Proc. of 4th International Conf. On Security and Privacy in communication networks, SecureComm '08, Istanbul, Turkey, 2008.

[19] F. Tseng, L. Chou, and H. Chao, "A survey of black hole attacks in wireless mobile ad hoc networks", Human-centric Computing and Information Sciences, Springer, Vol. 1, No. 4, pp. 1-16, 2011.

[20] S. Akansha and D. Rajni , "Wormhole Attack in Mobile Ad-hoc Network: A Survey", International Journal of Security and Its Applications, Vol. 9, No. 7, pp. 293-298, 2015.