Extended EAACK- An Secure Intrusion Detection System with Detection and Localization of Multiple Spoofing Attackers in MANET

Aditya P. Tapaswi[*], Pratik P. Nashikkar[*], Rohit S. Barge[*], Aniket M. Shinde[**], Prof. Pramod Patil [**]

[*] Department of Information Technology, Pune University., Students of Nutan Maharashtra Institute of Engineering and Technology, Pune, Maharashtra
[**] Assistant Professor, NMIET,Pune.

***Abstract*-** Invention of wireless network has brought up drastic change in networking. Mobile Ad hoc NETwork (MANET) has been evolved as one of the promising technology based on implementation of wireless network. Providing mobility, flexible infrastructure, fast and low cost deplyoment are the key features of MANET. MANET is being most widely used wireless technology has limited security against network attacks. Dynamic configurability adds flexibility to MANET but it makes it vulnerable to attacks like DoS, Wormhole, Man-In-Middle Attack, IP Spoofing Attacks. In this paper, we propose an intrusion detection system Extended Enhanced Adaptive ACKnowledgement (E-EAACK) which will detect the intrusion and localize the attacker. This system includes security components of prevention, detection and reaction. Specially designed for MANET, E-EAACK serves in detection of malicious behaviour without much affecting Network Performance. In addition it will detect and localize multiple IP Spoofing Attacks. We propose, the use of digital signature for authentication of nodes and S-ACK scheme for detecting anomalous behaviour in network. The implementation of GADE model for detection of attacks and IDOL framework for localization of the intruder makes E-EAACK a more effective security solution for MANET.

***Index Terms*-** MANET,EAACK, Digital Signature, GADE, IDOL.

I. INTRODUCTION

With constantly changing technology, people prefer to have information on their fingertips anywhere - anytime

Thus increasing in the use of wireless networks. MANET one of the promising technology in wireless networking has features like dynamic configurability, low cost of deployment. MANET does not need a fixed infrastructure[2]. MANET is dynamically configurable network in which nodes set up paths among themselves to transmit packets[1]. Without getting help of fixed infrastructure MANET forms self-configuring network by collection of mobile nodes. Transmitter and receivers both are equipped in a MANET node, so node can act as a Router and a Host at the same time.

There are two scenarios concerning topology in MANET. First, single-hop network where nodes within the radio communication range can directly communicate with each other; Second, Multi-hop network where nodes out-side each the range must depend on some other nodes to relay messages. Thus acting like a Router to relay mes-sages to other nodes outside each others range have to rely on some other nodes to relay messages.

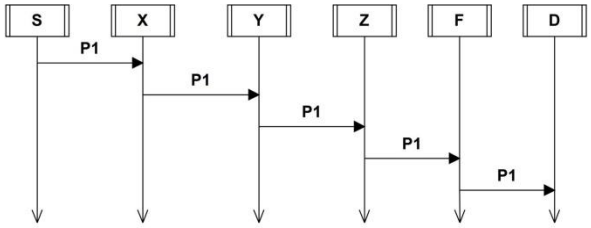

Figure 1: Relay of Messages in MANET

The Mobile Ad hoc Wireless Network is more vulner-able to be attacked than wired network. These vulnera-bilities exist due to the structure of MANET and are dif-ficult to remove. Attacks with malicious intent are made to exploit these loop-holes and to deteriorate the MANET operation. Attack prevention measures, such as authenti-cation and encryption, can be used as the primary defence mechanism for reducing the possibilities of attacks. How-ever, these techniques have some or the other limitations that are designed for a set of some known attacks. They are inefficient to prevent newer attacks that are designed for bypassing the existing security methods.

Due to the transparency of wireless networks, they are especially vulnerable to spoofing attacks where an attacker falsifies its identity to masquerade as another device, or even creates multiple illegal identities. Spoofing attacks are a serious threat as they represent a form of identity compromise and can facilitate a variety of traffic injection attacks, such as DoS attacks. It is thus desirable to detect the presence of spoofing and remove them from the net-work [6] [7].

II. RELATED WORK

Due to the limitations of most of MANET routing rules, nodes MANET are reluctant on other nodes cooperation to relay data. This dependency facilitates an attacker oppor-tunity to have its impact on network by compromising one or more nodes. To

tackle this problem, it arises the need of enhancing the security level of MANETs.

2.1 Watchdog:

Watchdog was designed to improve the throughput of network with the existence of malicious node. It works for detecting malicious node by constantly listening to its next hop transmission.

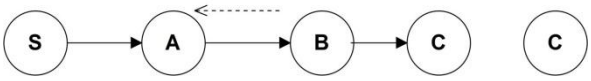

Figure 2: Operation in Watchdog

If the next hop fails to relay the packet ahead within certain period of time, it results in increment of failure counter. Furthermore, if failure counter exceeds a spe-cific threshold value, it reports network as misbehaving. Watchdog scheme fails in the following:

a. ambiguous collisions
b. receivers collisions
c. limited transmission power
d. false misbehaviour report
e. partial dropping[3]

2.2 TWOACK:

TWOACK [4]is neither an enhancement nor a Watch-dog based scheme. Aiming to resolve the receiver collision and limited transmission power problems of Watch-dog, TWOACK detects misbehaving links by acknowledging every data packets transmitted over each three consecutive nodes along the path from the source to the destination. Upon retrieval of a packet, each node along the route is required to send back an acknowledgement packet to the node that is two hops away from it down the route. TWOACK is required to work on routing protocols such as Dynamic Source Routing (DSR). The working process

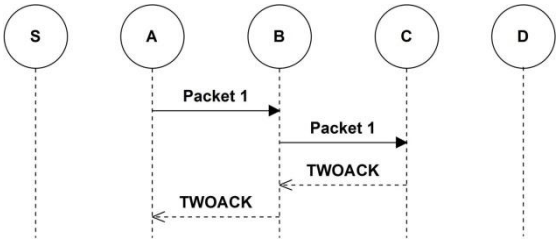

Figure 3: TWOACK scheme

of TWOACK is demonstrated figure, node a first forwards packet 1 to node B, and then node B forwards Packet 1 to node C. When node C receives Packet 1, as it is two hops away from node A, node C is obliged to generate a TWOACK packet, which contains reverse route from node A to node C, and sends it back to node A. The retrieval of this TWOACK packet at node A indicates the transmission of Packet 1 from node A to node C is successful. Other-wise, if this TWOACK packet is not received in a prede-fined time period, both nodes B and C are reported mali-cious. TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed by Watchdog. However, the acknowledgement process required in every packet transmission process added a significant amount of unwanted network overhead. Due to the limited battery power nature of MANETs, such redundant transmission process can easily degrade the life span of the entire network.

2.3 AACK :

It is a hybrid scheme which uses TWOACK for ac-knowledgement. AACK is acknowledgement based net-work layer scheme which consists a combination of schemes called TACK (similar to TWOAACK) and end-to-end acknowledgement scheme called ACKnowledgement . Compared to TWOACK, AACK significantly reduces net-work overhead, while still able to maintain or even out- shine the same network throughput[5]. In AACK, first

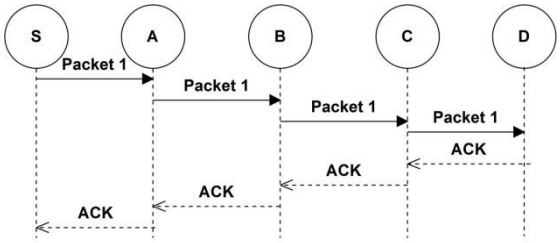

Figure 4: ACK scheme

the data transmit from source to destination. When the destination receives a packet it is required to send back an acknowledgement packet to source in the reverse route of the data packet. Within the specified time period if the source receives the acknowledgement packet, then the packet transmission is successfully. Otherwise, the source will switch to TACK scheme by sending a TACK packet. This hybrid scheme greatly reduces network traffic but is still unable to cope up with false misbehaviour report and forged acknowledgement.

2.4 Detecting spoofing attacks in mobile wireless environment:

Wireless network enables an attacker to masquerade as one of the device existing in network easily. This system proposes a method for detecting spoofing attack in mobile wireless environment. system develop the DEMOTE sys-tem which use of Received Signal Strength(RSS) traces collected over time without the knowledge of spatial constraint of the wireless node, utilizes temporal constraint to predict the best RSS. This approach does not require any changes or cooperation from wireless device other than packet transmission. By experiment from an office building environment system show that DEMOTE achieves ac-curate attack detection in both signal space as well as physical space using localization [9] [10] [11].

2.5 Detecting and Localization wireless spoofing attacks :

The system proposes both detection spoofing attacks as well as locating positions of attackers. System firstly works as a detector for wireless spoofing by using cluster analysis. Secondly, the system integrates the attack detector with real-time internal localization system which is also able to localize the positions of the attackers using point based algorithms. The

system has evaluated our method through investigation using both Wi-Fi network as well as

ZigBee network. Their result shows that it is possible to detect wireless spoofing with both high detection rate and low false positive rate[8].

III. System Description

The EEAACK system will consist of following techniques, model or mechanisms for intrusion detection and localization.

3.1 ACK

ACK is nothing but an end to end acknowledgment scheme. It acts as a crossbreed scheme in EEAACK. When there are no misbehaving nodes the transmission from source to destination is successful. Then destination sends an acknowledgement packet to source within predefined time constraint, otherwise source will switch to S-ACK mode[12].

3.2 S-ACK

Source sends S-ACK packet in the intention of detecting misbehaving nodes in the route. S-ACK sends acknowledgment back to source after the packet reaches consecutive three nodes ahead the route. The third node required to send a S-ACK acknowledgement to first node. S-ACK mode facilitates easy detection of misbehaving nodes in the presence of receiver collision and limited power for transmission[12].

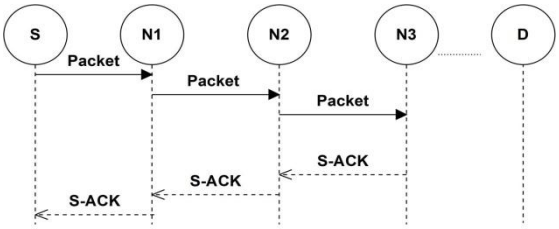

Figure 5: S-ACK scheme

N1, N2, N3 are three consecutive nodes. N1 sends S-ACK data packet to N2 which is next in the route and N2 relays it to N3. When N3 receives the S-ACK data packet it acknowledges N2 with S-ACK acknowledgement packet and N2 acknowledges back to N1. If N1 doesn't receive the acknowledgement within a particular time it will report N2, N3 as malicious nodes by generating a misbehaviour report. This misbehaviour report is sent back to the Source. To validate this report the source switches itself to MRA mode.

3.3 MRA

Misbehaviour Report Analysis (MRA)[12] is a scheme to confirm misbehaviour report generated in S-ACK mode. This report may be a false one as attacker may interfere in S-ACK scheme generating a false misbehaviour report. As a result, this may cause destruction of network by compromising guiltless nodes.

In MRA the source will check with the destination whether the destination node have received the missing packet through a different route. MRA mode is initiated by checking local knowledge base of sender for getting al-ternative route to destination; otherwise source uses Dy-namic Source Routing method for alternative route. Once the destination gets the MRA packet, it compares the MRA packet with the local knowledge base to verify if the re-ported packet was received by it. If received, then it in-forms the source that the misbehaviour report is false else it is considered as a legitimate report.

3.4 Digital Signature

All the above schemes are based on acknowledgement. These acknowledgements could be doubtful and must be checked for their rightfulness. We use digital signature in order to maintain integrity of the system. If we don't use digital signature the above discussed 3 schemes will be de-fenceless. We can use DSA or RSA algorithms to implement digital signature schemes.

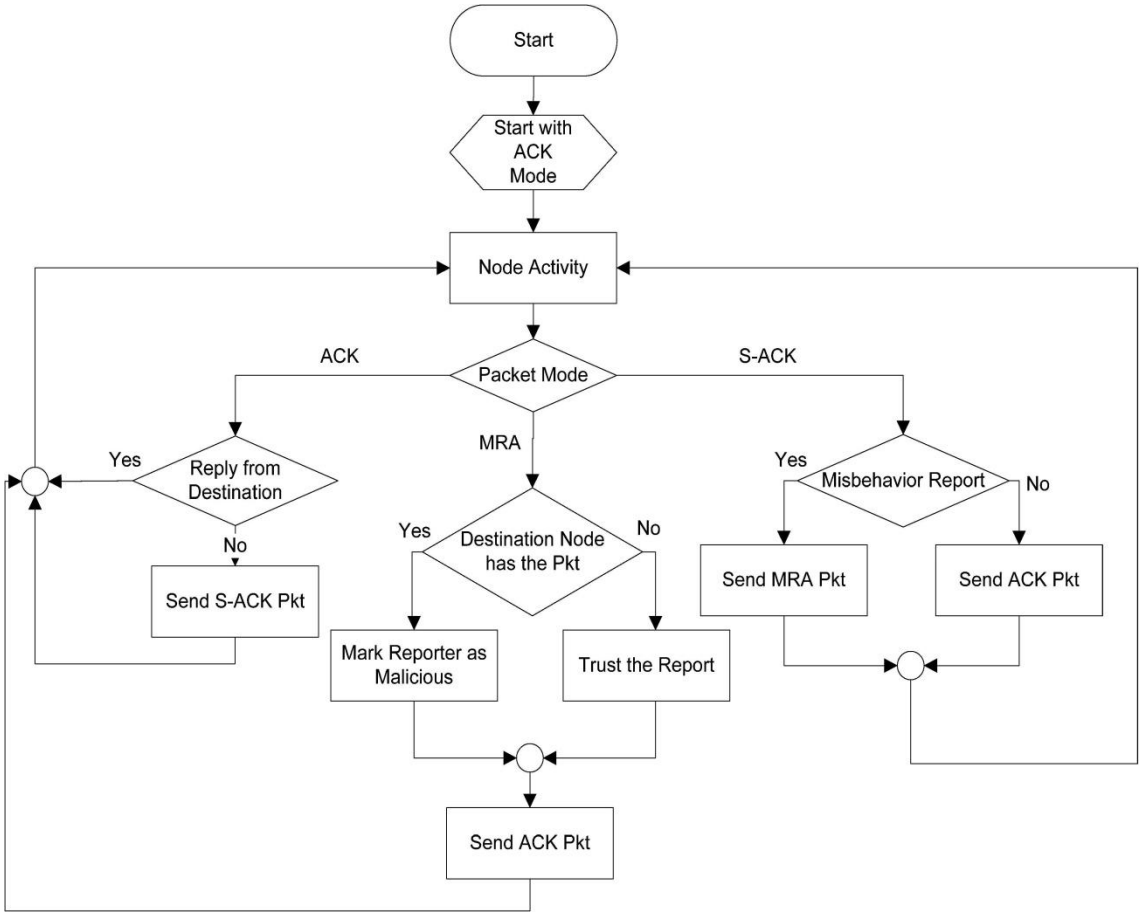

Figure 6: Detection

3.5 GADE

GADE stands for Generalize Attack Detection Model. It is attack detection method used in our system. There are two stages: First, attack detection; second, determine number of attackers. Attackers use transmission power of 10db to send packets, whereas original node uses 15db trans-mission power level observed according to the attributes in Received Signal Strength. RSS is a property correlated with location in physical space. The spoofing at-tacker used transmission power of 10 dB to send packets, whereas the original node used 15 dB transmission power levels. System observed that the curve of Dm under the different transmission power level shifts to the right indicating larger Dm values. System observes this difference be-tween power levels and detects attack effectively in GADE model[13].

GADE uses cluster analysis for attack detection. RSS readings from wireless nodes may fluctuate and they should be clustered together. The cluster analysis for attack detection, System presents the Receiver Operating Charac-teristic curves of using Dm as a test statistic to perform attack detection for both the 802.11 and the 802.15.4 net-works. The detection rate and false positive rate for both networks under different threshold settings. The results are encouraging, showing that for false positive rates less than 10 percent, the detection rate are above 98 per cent when the threshold is around 8 db. Even when the false positive rate goes to zero, the detection rate is still more than 95 per cent for both networks.

The estimation of the number of attackers will cause failure in localizing the multiple adversaries. As we do not know how many adversaries will use the same node iden-tity to launch attacks, determining the number of attackers becomes a multiclass detection problem and is similar to determining how many clusters exist in the RSS readings. The System Evolution is a new method to analyse cluster structures and estimate the number of clusters. The Sys-tem Evolution method uses the twin-cluster model, which are the two closest clusters among K potential clusters of a data set. The twin-cluster model is used for energy calculation.

The advantage of Silhouette Plot is that it is suitable for estimating the best partition. Whereas the System Evo-lution method performs well under difficult cases such as when there exists slightly overlapping between clusters and there are smaller clusters near larger clusters.

The training data collected during the offline training phase, we can further improve the performance of deter-mining the number of spoofing attackers. In addition, given several statistic methods available to detect the number of attackers, such as System Evolution and SILENCE, system can combine the characteristics of these methods to achieve a higher detection rate. This mechanism explores Support Vector Machines to classify the number of the spoofing at-tackers.

3.6 IDOL:

Integrated detection and Localization Framework[13] IDOL framework used to localize multiple attackers. IDOL efficiently detects attackers using different transmission power mechanism. The mainstream method of averaging RSS readings cannot differentiate RSS readings from different location and thus is not viable for localizing the attackers. This framework uses RSS medoids returned from SILENCE as input to localization algorithms to estimate the positions of intruders. In order to efficiently implement IDOL we use following algorithms:

a. RADAR-gridded: For localizing adversaries this algo-rithm uses RSS readings and nearest neighbour matching technique in single space, to localize the attacker.
b. Area-Based Probability: ABP incorporates signal map. Experimental area is split into regular grid to equal size ac-cording to RSS reading observed for that particular grid. c. Bayesian Networks: BN uses signal to distance propa- gation model (multilateration) to localize the attacker.

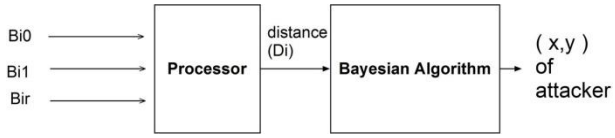

Figure 7: Working of BN

IV. Conclusion

Packet Dropping and Identity based attacks have always been main threats to MANET. In this paper, we proposed a fully equipped system named E-EAACK primarily in-tended for MANET and made it efficient in comparison to other popular mechanisms. It also overcomes the issues in MANET such as limited transmission power, receivers collision and false misbehaviour report.

We also propose the use of RSS based spatial correlation associated with each node that is hard to falsify for detecting identity based attacks. Our system can do both, detect the attack and decide the number of invaders and exclude them.

References

[1] L. Buttyan and J. P. Hubaux, Security and Cooperation in Wireless Networks. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.

[2] G. Jayakumar and G. Gopinath, Ad hoc mobile wire-less networks rout-ing protocolA review, J. Comput. Sci., vol. 3, no. 8, pp. 574582, 2007.

[3] S. Marti, T. J. Giuli, K. Lai, and M. Baker, Mitigat-ing routing misbe-haviour in mobile ad hoc networks, in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., Boston, MA, 2000, pp. 255265.

[4] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, An acknowledgment-based approach for the detection of routing misbe-haviour in MANETs, IEEE Trans. Mobile Comput., vol. 6, no. 5, pp.536550, May 2007.

[5] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, Video transmission enhancement in pres-ence of misbehaving nodes in MANETs, Int. J. Multi-media Syst., vol. 15, no. 5, pp. 273282, Oct. 2009

[6] D. Faria and D. Cheriton, Detecting Identity-Based At-tacks in Wireless Networks Using Signalprints, Proc. ACM Workshop Wireless Security (WiSe), Sept. 2006.

[7] Q. Li and W. Trappe, Relationship-Based Detection of Spoofing-Related Anomalous Traffic in Ad Hoc Net-works, Proc. Ann. IEEE Comm. Soc. on IEEE and Sensor and Ad Hoc Comm. and Networks (SECON), 2006.

[8] Y. Chen, W. Trappe, and R.P. Martin, Detecting and Localizing Wireless Spoofing Attacks, Proc. Ann. IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON), May 2007.

[9] P. Bahl and V.N. Padmanabhan, RADAR: An in-Building RF-Based User Location and Tracking Sys-tem, Proc. IEEE INFOCOM, 2000.

[10] E. Elnahrawy, X. Li, and R.P. Martin, The Limits of Localization Using Signal Strength: A Compara-tive Study, Proc. IEEE Intl Conf. Sensor and Ad Hoc Comm. and Networks (SECON), Oct. 2004.

[11] Y. Chen, J. Francisco, W. Trappe, and R.P. Martin, A Practical Approach to Landmark Deployment for In-door Localization, Proc. IEEE Intl Conf. Sensor and Ad Hoc Comm. and Networks (SECON), Sept. 2006.

[12] EAACK A Secure Intrusion-Detection System for MANETs Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, Member, IEEE.

[13] Detection and Localization of Multiple Spoofing At-tackers in Wireless Networks Jie Yang, Student Mem-ber, IEEE, Yingying (Jennifer) Chen, Senior Member, IEEE, Wade Trappe, Member, IEEE, and Jerry Cheng.

Authors

First Author – Aditya P. Tapaswi, Department of Information Technology, Pune University., Students of Nutan Maharashtra Institute of Engineering and Technology, Pune, Maharashtra
Second Author – Pratik P. Nashikkar, Department of Information Technology, Pune University., Students of Nutan Maharashtra Institute of Engineering and Technology, Pune, Maharashtra
Third Author – Rohit S. Barge, Department of Information Technology, Pune University., Students of Nutan Maharashtra Institute of Engineering and Technology, Pune, Maharashtra
Fourth Author – Aniket M. Shinde, Department of Information Technology, Pune University., Students of Nutan Maharashtra Institute of Engineering and Technology, Pune, Maharashtra