ISSN:0975-9646

Proof-Based Intrusion Detection System in MANETs

[1]Nimmy.S
P G Scholar
Computer Science & Engineering
Mangalam College of Engineering
Ettumanoor, Kerala, India

[2] Sreenimol K.R
Associate Professor
Computer Science & Engineering
Mangalam College of Engineering
Ettumanoor, Kerala, India

***Abstract*— The source node forwards packet to destination node through intermediate nodes in MANETs. While forwarding packets, a node can simply claim it has not received the packet from previous node or it has forwarded the packet to next node without actually doing so. That is some nodes or a node is misbehaving here. To address these issues a token-based scheme called Proof-Based Intrusion Detection System in MANETs is proposed here.**

***Keywords*— Proof-Based Intrusion Detection System, Mobile Adhoc Network (MANET), Digital Signature (RSA), Digital Signature Algorithm (RSA).**

I. INTRODUCTION

Many schemes have been discussed in the past, like Watchdog, TWO-ACK and MRA regarding Intrusion Detection System in MANETs. But none of the earlier discussed schemes have addressed a clear-cut solution for handling the malicious nodes. Here have proposed a Proof-Based Intrusion Detection System which detects two of the major issues which couldn't be solved by the previous schemes, mainly when two intermediate nodes seem to be suspicious. Need to find which one is malicious and get rid of it. The integrity of source node and message id of the packet forwarded is ensured using RSA. Trust value is also computed based on nodes past history. The one with highest value is trusted most.

II. DIFFERENT SCHEMES

A. WATCHDOG

Watchdog consists of two parts, mainly Watchdog and Pathrater. Watchdog acts as IDS in MANETs. It is used to detect malicious nodes by watching next hop's transmission. When it reaches a limited period of time, the failure counter set is increased. When the counter reaches out of already defined threshold, Watchdog reports it as malicious. At that time, Pathrater cooperates with the routing protocols in order to get rid of these malicious nodes from future transmissions. But this scheme proves inefficient in the presence of collisions, transmission power, false misbehaviour report, collusion and packet dropping.

B.TWOACK

TWOACK detect misbehaving links by acknowledging each data packet that is transmitted over every three consecutive nodes in the path from source to destination. On retrieval of a data packet every node has to send back an acknowledgement packet to the node that is two hops away from it. Even though TWOACK solves receiver collision and limited transmission power problems, it produces network overhead due to the acknowledgement process.

C.MRA

This scheme is used to detect malicious nodes in the presence of false misbehaviour report. But these reports can be generated by malicious attackers to falsely report trusted nodes as malicious. In that cases the source node searches for an alternate route to destination. Once the destination node receives MRA packet, it searches local knowledge base and checks whether the reported packet was received. If it was already received then it is a false misbehaviour report and those who generated it is reported as malicious. Or else the report is trusted and accepted. But still if two nodes are suspected, to find which one is malicious this scheme is not sufficient. So adopted a Proof-Based scheme for detecting malicious nodes.

III. PROPOSED WORK

A. *PROOF-BASED INTRUSION DETECTION SYSTEM*

In this infrastructure of MANETs, each node forwards packets to the neighbouring node till it reaches the destination node. Each time a packet is forwarded that node's trust value is increased by 1 count. The packet is forwarded using proof, which contains source message id and the route (that is from source to which node it is been forwarded).The message id is encrypted using RSA algorithm. This is done using source's private key. Proof cannot be generated automatically at the same time it can only be decrypted by the source node. The integrity of source node is also ensured using RSA. The route for sending packets is selected using DSR (Dynamic Source Routing) routing protocol. The packet is forwarded from source to the neighbouring node. Again it is forwarded to next node in the route. When it reaches the third node.an acknowledgement is to be send back to the source. At the same time, upon receiving the packet a proof is to be generated by the receiving node. This process is continued till the packet reaches destination node. In case the packet is missed in between, say node A forwards packet to node B using node A's message id and route, that is from A to B.

Once B receives the packet, it generates a proof using A's message id and the route is from B to C.C now has to send an acknowledgement packet back to A after generating the proof. Here we are using THREEACK scheme. Similarly C forwards packet to D. Suppose D is the destination, on receiving the packet D generates a proof and sends acknowledgement packet to A. Meanwhile the trust value of each node increments as it forwards packets each time. Suppose A forwarded packet to B and B to C. But C says it didn't get packet from B or it got packet but it didn't forward to D, but simply says C forwarded to D. In this case we have to find out which one is malicious, C or D or both. Now will check who all has generated proof .If B has generated proof then we can get that B is not malicious. Then check for C. If C has not generated proof then get to know that it is malicious. Again check for D's proof. If it has got packet from some other node than C or its trust value is higher than C then D is trusted and C is reported as suspicious. Now remove C for further communication until C's nature changes.

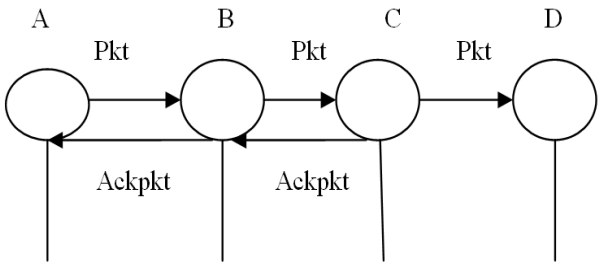

Figure 3.THREEACK scheme: Upon three hops the node is to send back acknowledgement packet to source node.

IV. Result And Analysis

Here analyse the accuracy of detection of malicious nodes and success rate of the system. As compared to previous schemes the proposed scheme proves to give a better result as shown in graph 4.1 and 4.2.

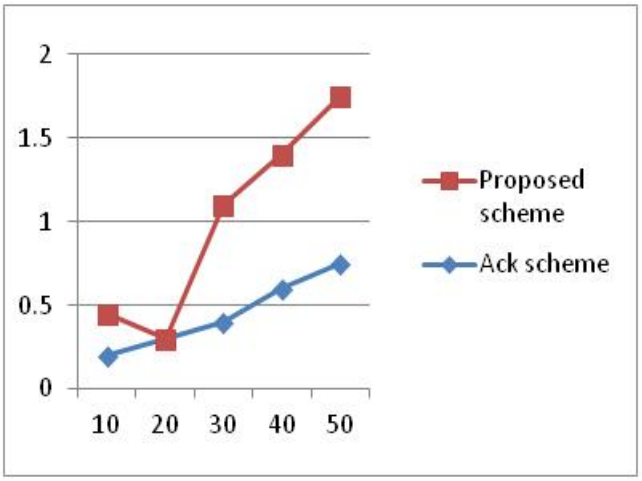

Fig.4.1 Number of nodes vs Accuracy of detection.

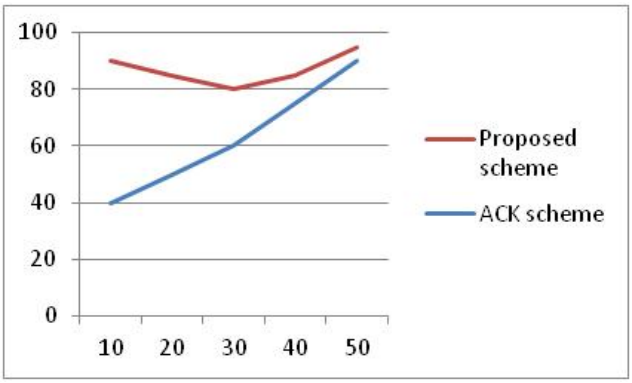

Fig.4.2 Number of packets vs Success rate.

Simulation done using one SIM and graphs are been plotted in terms of performance analysis.

V. Conclusion And Future Work

A. *Conclusion*

Have discussed about various schemes of Intrusion detection systems in MANETs, its advantages and disadvantages. Also have discussed about Proof-Based Intrusion Detection System in MANETs. Proposed scheme is a token-based one which addresses the issues of detecting malicious nodes specially when a node simply says it has not received a packet that is forwarded , at the same time it says it forwarded the packet to neighboring node without actually doing so. The integrity of source is ensured using RSA.

B. *Future Work:*

To address the above discussed issues which are drawn in this work, which one to be solved first based on reducing overhead; a system is not yet got. Would like to focus on this issue in the future.

References

[1] K. Al Agha, M.-H. Bertin, T. Dang, A. Guitton, P. Minet, T. Val, and J.-B.Viollet, "Which wireless technology for industrial wireless sensor networks?The development of OCARI technol," IEEE Trans. Ind. Electron., vol. 56, no. 10, pp. 4266–4278, Oct. 2009.

[2] R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad hoc Network Security," in Lecture Notes in Electrical Engineering, vol. 127.New York: Springer-Verlag, 2012, pp. 659–666.

[3] R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hocnetworks: A survey," in Proc. 2nd Int. Meeting ACCT, Rohtak, Haryana,India, 2012, pp. 535–541.

[4] T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," in Wireless/Mobile Security. New York: Springer-Verlag, 2008.

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

[6] D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, and L. Benini, "Modeling and optimization of a solar energy harvester system for self-powered wireless sensor networks," IEEE Trans. Ind. Electron., vol. 55, no. 7,pp. 2759–2766, Jul. 2008.

[7] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks:Challenges, design principles, and technical approach," IEEE Trans. Ind.Electron., vol. 56, no. 10, pp. 4258–4265, Oct. 2009.

[8] Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hocnetworks," in Proc. 4th IEEEWorkshop Mobile Comput. Syst. Appl., 2002, pp. 3–13.

[9] Y. Hu, A. Perrig, and D. Johnson, "ARIADNE: A secure on-demand routing protocol for ad hoc networks," in Proc. 8th ACM Int. Conf. MobiCom,Atlanta, GA, 2002, pp. 12–23.

[10] G. Jayakumar and G. Gopinath, "Ad hoc mobile wireless networks routing protocol—A review," J. Comput. Sci., vol. 3, no. 8, pp. 574–582.