A Secure Intrusion Detection System for MANETs using MAES

Poonam R. Singh[1], Srushti Soni[2]

[1]Research Scholar, Electronics & Communication Department, Parul Institute of Engineering & Technology, Gujarat,
[2] Assistant Professor, Electronics & Communication Department, Parul Institute of Engineering & Technology, Gujarat, India

ABSTRACT

Wireless Networks are being preferred nowadays over wired networks because it is mobile. Hence it is used in many fields. The most important application of wireless network is Mobile Ad hoc NETwork (MANET) .In MANET all the nodes works as both transmitter and receiver. MANETs are used in various fields like military, industry and emergency recovery. But there is a certain drawback in MANETs, that it becomes prone to malicious attacks very fast. To avoid such attacks, we need a good intrusion detection and prevention system. This system is named as Enhanced Adaptive ACKnowledgement (EAACK). EAACK gives better malicious- behaviour -detection than the traditional approaches. Using Modified Advanced Encryption system MAES with EAACK, better results are obtained as it provides more security.

Keyword: - *Mobile Ad hoc Network; Modified Advanced Encryption System; Advanced Encryption System; ;False Misbehaviour Report*

---

1. INTRODUCTION

In today's life wireless networks are much easier to use rather than wired network. As wireless network is having more mobility and scalability it is used every now and then. Wireless ad-hoc network consists of a collection of "peer" mobile nodes that are capable of communicating with each other without help from a fixed infrastructure [1]. By definition, Mobile Ad hoc NETwork is a continuously self - configuring, infrastructure-less network of mobile devices connected without wires [2]. MANET consists of mobile nodes. This mobile node has wireless transmitter and receiver which can communicate with each other in two ways, directly or indirectly. If our nodes or components are not within same range we can use MANET. But to achieve this MANET is divided into two networks, namely single-hop and multi-hop. In single-hop network, nodes which are within same range can communicate with each other directly, But, in multi-hop network, we use intermediate nodes to communicate with each other to transfer data, if we cannot communicate with each other directly.

Due to MANET centralized network it is self-configuring and self-maintaining. Due to such features of MANETs, they are used in application such as military conflict, human induced disasters and medical emergency recovery. Enforcing policy is difficult because they lack infrastructure. Due to node's physical protection, malicious attackers can easily attack the nodes. In network, routing table is maintained. In MANET, routing protocol assumes that every node in network cooperates with each other and there is no malicious node present in the network. Attackers can easily attack the network and can easily insert malicious nodes or non-co-operative nodes into the network. Due to distributed architecture of MANET, it is difficult to centralize a monitoring technique for MANET. In this case, it is difficult to develop an intrusion detection and prevention system for MANETs.

2. ENHANCED ADAPTIVE ACKNOWLEDGEMENT ALGORITHM

Shakshuki [3] et al proposed an IDS EAACK, consists of three parts namely ACK, Secure Ack (S-ACK), and Misbehavior Report Authentication (MRA) which is designed to overcome above three problems such as limited transmission power, receiver collision and false misbehavior report.

Node S first sends out an ACK data packet to the destination node D. After receiving the packet node D is required to send back an ACK acknowledgment packet along the same route but in a reverse order. Within a predefined time period, if node S receives ACK, then the packet transmission from node S to node D is successful.

In S-ACK mode, every three consecutive nodes work in a group to detect misbehaving nodes. Node A first sends out S-ACK data packet to node A. Then, node B forwards this packet to node C. When node C receives the packet, as it is the third node in the group, node C is required to send back an S-ACK acknowledgment packet to node B. Node B forwards the packet back to node A. If node A does not receive this acknowledgment packet within a predefined time period, both nodes B and C are reported as malicious. Finally, a misbehavior report will be generated by node A and sent to the source node S.

In MRA mode, Source node S will check its knowledge base for an alternative route to reach the destination node D. Source node S will send an MRA packet to node D using alternative path. When the destination node receives an MRA packet, it searches its knowledge base and compares if the reported packet was received. If it is already received, then it is safe to conclude that this is a false misbehavior report and whoever generated this report will be marked as malicious. Otherwise, the misbehavior report is accepted.

All the 3 modes of EAACK, namely ACK, S-ACK, and MRA are acknowledgement based detection schemes. If the attackers are able to forge these acknowledgement packets, then all of the three schemes will become vulnerable. Thus, it is very essential to ensure that all acknowledgment packets in EAACK are authentic.

3. Modified Advanced Encryption System: The Algorithm begins with an Add Round Key followed by 9 rounds of four stage and a 10^{th} round of 3 stages. This applies for both Encryption and Decryption with the exception that each stage of a round the Decryption Algorithm is the counterpart of the inverse of its Encryption Algorithm. The four stages in Encryption are:1) Substitute Bytes 2) Shift Rows 3) Mix Columns 4) Add Round Key.

The 10^{th} round simply leaves out the Mix Column stage. The first 9 rounds of the decryption algorithm is the inverse of the four stages in encryption algorithm. The 10^{th} round simply leaves out the Mix Column stage

4. False Misbehaviour Behaviour: Node A sends Packet1 to Node B. As Node B receives Packet1 it immediately sends Packet1 to Node C. Now Node A gets to know that Node B has successfully forwarded the packet to Node C, still Node A sends false report to the source node or previous node that Node B is misbehaving. This is known as false misbehaviour report.

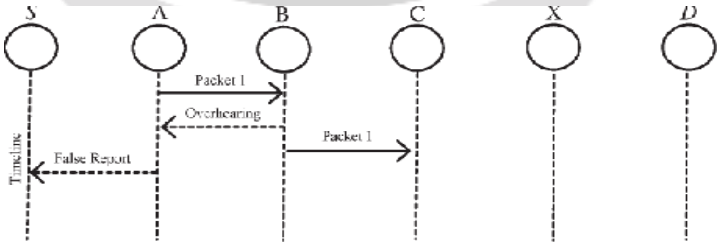

Fig 1. False Misbehaviour Report[1]

5. Results

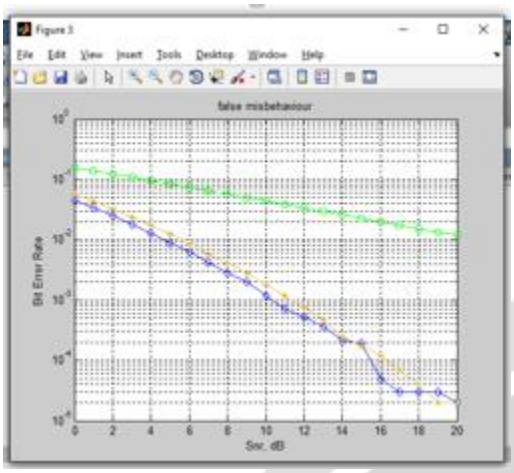

Fig 2: Detection of FMR Attack in terms of BER in both proposed and existing scheme

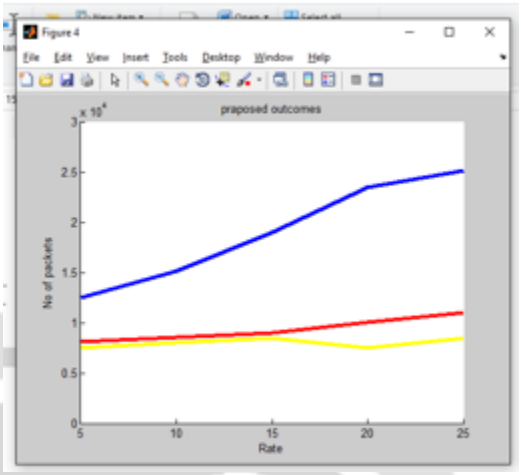

Fig 3: Comparison of proposed work with existing system and the system performance after removal of FMR Attack

Fig 2 shows the detection of False Misbehaviour report and its effect on proposed work and existing hybrid approach using AES, RSA and MD5 in terms of Bit Error Rate. We can see that FMR is detected and corrected so BER is maintained till 16 nodes but it is disturbed as the node increases after 16.Fig 3 shows the comparison of the False Misbehaviour Attack (FMR) to the proposed work EAACK using MAES and with hybrid cryptography approach using AES, RSA and MD5.In this figure we can clearly see that our proposed system MAES gives more accuracy in terms of no of packets transferred.

6. Conclusion:

We conclude from the results that accuracy increases in our proposed work i.e EAACK using MAES as no of packets transferred increases. We also conclude that FMR Attack can be solved and system performance can be increased to certain extend but it decreases as the number of nodes increases. Time Delay can also be reduced as the packets transferred are within the nodes which are authenticated using MAES.

7. ACKNOWLEDGEMENT

I would like to express my deepest appreciation to my guide Prof. Srushti Soni, Electronics and communication department, Parul institute of engineering and technology for her continuous assistance, motivation, and persistent support in regards to this research work. Without their supervision and constant help this dissertation would not have been possible.
I would like to thank all faculty members of Electronics and Communication Department for their help and guidance. They have been great sources of inspiration to me and I thank them from the bottom of my heart. Last but not least I would like to thank my parents, who taught me the value of hard work by their own example. They rendered me enormous support being apart during the whole tenure of my study in PIET Vadodara.

8. REFERENCES

[1]Poonam Joshi,Pooja Nande,Ashwini Pawar, Pooja Shinde, Rupali Umbare,"EAACK-A Secure Intrusion Detection and Prevention System for MANETs", IEEE 2015 International Conference on Pervasive Computing(ICPC).

[2] M.Vijay, R.Sujatha , "Intrusion Detection System To Detect Malicious Misbehaviour Nodes In MANET",IEEE 2014 ICICES(International Conference on Information Communication & Embedded Systems).

[3] Elhadi M. Shakshuki, Nan Kang,Tarek R. Sheltami, "EAACK-A Secure Intrusion-Detection System for MANETs", IEEE Transactions on Industrial Electronics,VOL.60,NO.3,March 2013.

[4]T.Archana, Mr.N.Rajkumar, "Enhanced Acknowledgement Based Intrusion Detection for Manets", IEEE 2014 ICICES (International Conference on Information Communication & Embedded Systems).

[5]Sivaranjini S, Rajashree S, "Secure Data Transfer in MANET Using Hybrid Cryptosystems", IEEE 2014 ICICES (International Conference on Information Communication & Embedded Systems)

[6] Ankur O. Bang, Prabhakar L. Ramteke,"MANET : History, Challenges And Applications", IJAIEM ,Volume 2, Issue 9, IEEE September 2013.

[7]N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowledgements in MANETs," in Proc. IEEE 25th Int. Conf. AINA, Biopolis, Singapore, Mar. 22-25, 2011, pp. 488–494.

[8]N. Nasser and Y. Chen, "Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network," in Proc. IEEE Int. Conf. Commun., Glasgow, Scotland, Jun. 24–28, 2007, pp. 1154–1159.