International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Survey on Novel Hybrid Techniques in EAACK for Prevention of Attacks in MANET'S

Pranita Prakash Kulkarni

Pune University, Department of Computer Engineering, Zeal College of Engineering & Research, Narhe, Pune- 411041, India

Abstract: ***Wireless network are used very rapidly. Mobile ad hoc network (MANET) is one of the most important applications of wireless networks in which nodes present in the system work individually. In this paper, we have proposed a system, which can provide high security when data is send from source to destination. The system is called as Hybrid Cryptography. Hybrid Cryptography gives a better security than any other traditional approaches. In existing system less security provider is used. In this paper, to reduce network traffic, packet delivery ratio caused by existing system, we are using digital signature based RSA and DES algorithm. Compared to present approaches, Hybrid Cryptography demonstrates higher malicious behavior detection rates in certain states while does not greatly affected the network performances.***

Keywords: Enhanced Adaptive Acknowledgement (EAACK), Mobile Ad-hoc Network (MANET), Packet Delivery Ratio (PDR), Received Signal Strength (RSS).

1. Introduction

Mobile Ad hoc NETwork (MANET) is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. Industrial remote access and control via wireless networks are becoming more and more popular these days .One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility. However, this communication is limited to the range of transmitters. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own. MANET solves this problem by allowing intermediate parties to relay data transmissions. This is achieved by dividing MANET into two types of networks, namely, single-hop and multihop. In a single-hop network, all nodes within the same radio range communicate directly with each other. On the other hand, in a multihop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range. In contrary to the traditional wireless network, MANET has a decentralized network infrastructure. MANET does not require a fixed infrastructure; thus, all nodes are free to move randomly MANET is capable of creating a self-configuring and self-maintaining network without the help of a centralized infrastructure, which is often infeasible in critical mission applications like military conflict or emergency recovery. Minimal configuration and quick deployment make MANET ready to be used in emergency circumstances where an infrastructure is unavailable or unfeasible to install in scenarios like natural or human-induced disasters, military conflicts, and medical emergency situations

2. Literature Survey

Elhandi M. Shakshuki, Nan Kang, Tarek R. Sheltami, author describe various intrusion detection in MANETs and its drawbacks. EAACK helps for solving false misbehavior report problem and bring some new technique, which are identified with the enhanced adaptive acknowledgement. The methods, which are utilized, analyses the problem of ACK, TWO ACK and Watchdog scheme. The techniques depend on acknowledged packets; Digital Signature is used for preventing from attacker block from attacking the packets [1]. The author has represent the security which is depend on the acknowledgements packets, that how to shielded those packets from attacks and clarify intrusion detection system scheme for MANETs. Development which expands a minor in network overhead, utilizing EAACK2 which is called as enhanced adaption of EAACK, EAACK2 which implement better in the existence of false misbehavior and partial dropping not just do a superior execution in the presence of forged acknowledgement packets, but also empower the packets purity when potential attack happen [2]. The author additionally had an arrangement to inspect other confirmation plan and check out the performance in the algorithm. Because of this, memory space of mobile nodes keeps better battery. It gives description about the capability of the protocols to modify both malicious and benign faults grants fast and reliable data carrying in highly adverse network situation and examined various protocols like Secure Message Transmission (SMT), Secure Single Path (SSP), Transmission control protocol (TCP), Stream Control Transmission Protocol (SCTP) [3] MANETs are distributed is Intrusion Detection System. and explains about the features of EAACK that the system consist of a powerful attack control, which can help to guarantee the data security. Once the activator characterizes the keys to the nodes, automatically the preferences will be generated. And also explain that how they can detect as well as prevent from the malicious attacks [4][5]. Fast and secure data transmission in mobile ad hoc network using proactive and reactive system. In this paper, author uses the process algorithm and central agent for giving the security to the network. The disadvantage of proactive protocol is to wait for a new node when it is added to the network, it takes some time to concentrate. For avoiding this drawback, reactive protocol is used. It increases the time efficiency and data transfer rate also increases [7][8].

3. Proposed System

Source node is used to send packets to the number of destination nodes therefore the activated path can be anyone. When packet is sent from the source node to the next node then back acknowledgement is sent to the source node, which is also called as activation node. When packet is sent from them next node then back acknowledgement is directly sent to the source node. When provided packet, text, data is reached at destination node then destination node sent .

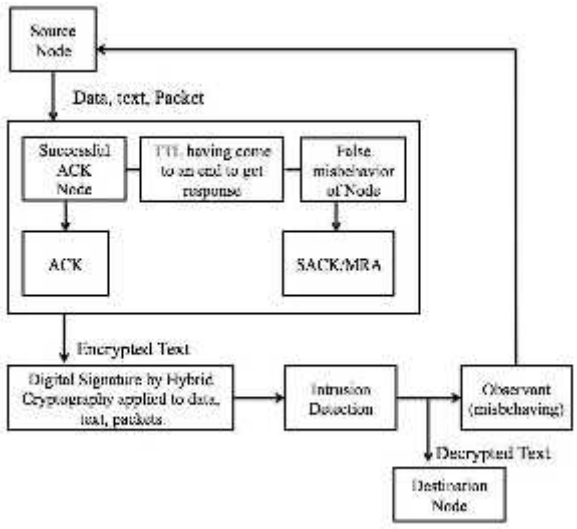

Figure 1: System Architecture

acknowledgement directly to the source node. At the same time, the text, data, packet is encrypted with digital signature at the source node. When data, text, packet is reached at destination node then packet, text, data, is decrypted at original message i.e., text, data, packet.

Proposed system makes uses of Hybrid cryptographic technique using RSA approach. RSA stands for the name of the three researchers who designed it, Ron Rivest, Adi Shamir ,Leonard Adleman. Factorization of two major prime numbers is utilized as a part of RSA.

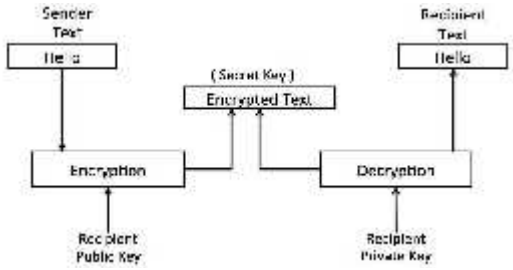

Figure 2: Working Of RSA

Public key are being utilized as a part of RSA for secure Transmission of data. The required key for the data encryption is public and the required key for data decryption is private which is shown in figure

4. Conclusion

The most discussed field when MANET's are concerned is the Intrusion Detection System. Intrusion Detection System, which basically concentrates on preventing attacks, which come from the attacker in the network, which can be harmful to the system. At the point when security issues are seen then packet dropping and hacking is the most important concern in MANET's. For that we have given IDS named Hybrid Cryptography with some new techniques and methods for prevention of attacks. There are some important features in the system:

1) This system has a powerful prevention control, which is one of the important and necessary conditions to guarantee the security of the data.
2) By providing Hybrid Cryptography technique, it will become difficult for attacker to break the network as well as retrieved the data. We can extend our work in future that not using any kind of trusted third party (TTP) for key administration and could be recognized different attacks

References

[1] Elhadi M. Shakshuki, IEEE, Nan Kang, and Tarek R. Sheltami, EAACK—A Secure Intrusion-Detection System for MANETs. IEEE Trans. on industrial Electronics vol. 60, No. 3, ,pp. 1089-1098, 2013
[2] N. Kang , E. Shakshuki and T. Sheltami, "Detecting misbehaving nodes in MANETs", Proc. 12th Int. Conf. iiWAS, pp. 216-222, 2010.
[3] 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.
[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] V 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.
[6] 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, 2009
[7] K. Liu , J. Deng , P. K. Varshney and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehaviour in MANETs", IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536-550, 2007
[8] J. Parker , J. Undercoffer , J. Pinkston and A. Joshi, "On intrusion detection and response for mobile ad hoc networks", Proc. IEEE Int. Conf. Perform., Comput., Commun., pp. 747-752, 2004.

Author Profile

Pranita P Kulkarni Student at Zeal Education Societys, Zeal college of Engineering and Research, Department of Computer engineering, pune-411046,India.