International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 07 | July-2016 www.irjet.net p-ISSN: 2395-0072

NOVEL HYBRID TECHNIQUES IN EAACK FOR PREVENTION OF ATTACKS IN MANET'S

Pranita Kulkarni

Department of Computer Engineering Shri Savitribai Phule Pune University, 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.*

***Key Words*: 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 BACKGROUND

With the customize technology, we are observing the expansion of MANETs into commercial application. So it is important to address its security issues. Such as existing IDSs in MANETs are

1) Watchdog

2) TWOACK and

3) AACK.

4) Digital Signature

Watchdog

Watchdog[1] improves the network throughput even in the presence of attackers. It contains two parts namely Watchdog and Path rater. It detects malicious nodes by hearing next hop's transmission. A failure counter is initiated if the next immediate node fails to forward or send the data packet. When the counter value exceeds a predefined threshold, the node is marked as malicious node. The major drawbacks are 1) Ambiguous collisions 2) limited transmission power 3)receiver collisions 4) false misbehavior report 5) partial dropping 6) collusion.

TWOACK

TWOACK[5] overcomes the receiver collision and limited transmission power limitation of Watchdog. Here acknowledgment of each and every data packet over every three consecutive nodes is sent which is from source to

destination. If ACK is not received in a predefined time, the remaining two nodes are marked as malicious. The major drawbacks are 1) Increased overhead 2) Degrades the life span of entire network. 3) Limited battery power

AACK

Adaptive acknowledgement(AACK)[3] is the combination of ACK and TWOACK. Source node sends packet to every node till packet reaches the destination node. Once packet reaches to destination, receiver node sends an ACK in the reverse order. If ACK is not received within fix interval of time , it switches to TWOACK scheme. The major drawbacks is that it suffers from 1) Forged acknowledgment packets. 2) False misbehavior.

Digital signature

Digital signature[2] is extensively used approach to ensure the integrity, authentication, and no repudiation of MANETs. All algorithms are based on acknowledgment except watchdog. Hence, it should be authenticated through digital signature.

3. SYSTEM ARCHITECTURE

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 the 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 back 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.

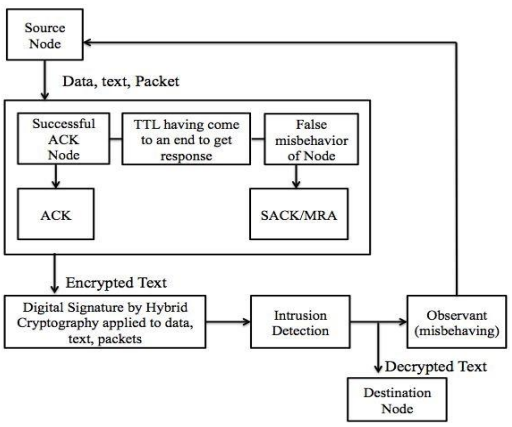

Figure 1 :System Architecture.

3.1 Implementation Details

Hybrid Cryptography with 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.

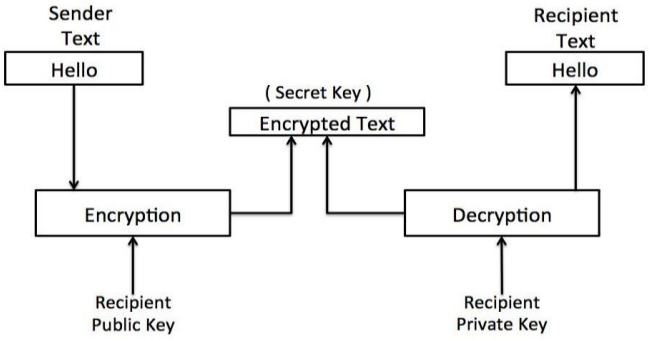

Figure: 2. Working of RSA

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 2.

RSA algorithm:

1) Select two major prime numbers x and y.

2) For security guidance, the integers x and y which are chosen consistently at odd and should be of similar bit.

3) Compute m, such that the modules for both the private and public key i.e. m=xy.

4) Compute ϕ= (x-1)(y-1).

5) Randomly choose an odd integer t such that t<ϕ and such that t and ϕ comparatively prime.

(gcd(t,k)=1) Where t is released as the public key exponent

6) The formula of generating decryption key is dk=t-1 mod ϕ

7) The pair by public key (t,k) and private key is dk.

RSA also named as “Public key Cryptography” which generally works with two keys i.e. public key as well as the private key. From the above algorithm, two keys are used and generated which is accessible to everyone is public key which is mutual key whereas

not accessible to everyone is private key which is not a mutual key. RSA also named as "Public key Cryptography" which generally works with two keys i.e. public key as well as the private key. From the above algorithm, two keys are used and generated which is accessible to everyone is public key which is mutual key whereas not accessible to everyone is private key which is not a mutual key.

4. RESULTS

PDR (Packet Delivery Ratio):
PDR[4] is described as the ratio of number of packets received by receiver at destination node to the number of packets sends by the source node.
PDR= Total amount of data packet received (Receiver) / Total amount of packet sent (Source)

RO or OFR (Routing Overhead or Overflow rate)[4]: This describes as the ratio of routing, which is related to the packets in bytes to the total routing and data transmission (sent or forwarded packets) in bytes.

RO = S (Routing Transmission) / (S(Data Transmission)+ S(Routing Transmission)).

Consider following Simulation Parameter table which contains Number of Nodes, Simulation Area, Mobility Nodes, Speed Range and Packet Size.

Parameter	Value
Number of Nodes	15 nodes
Simulation area	500 meter * 500 meter
Mobility Model	Dynamic Mobility
Speed range	Uniformly distributed (1-15) meter/second
Packet size	512bytes

Figure: 3. Simulation Parameter Table

4.1 Screenshots:

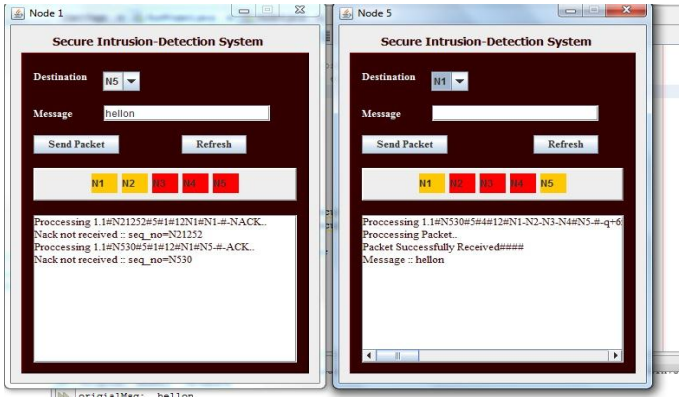

Figure: 4. Packet Transfer

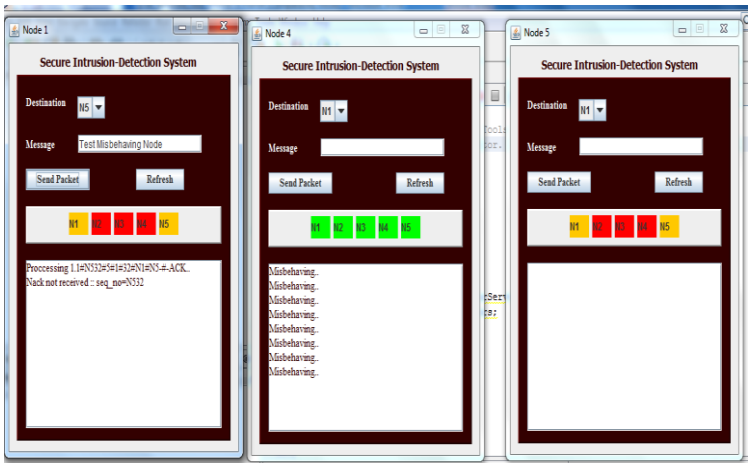

Figure: 5. Misbehavior Node

4.3:Performance Analysis

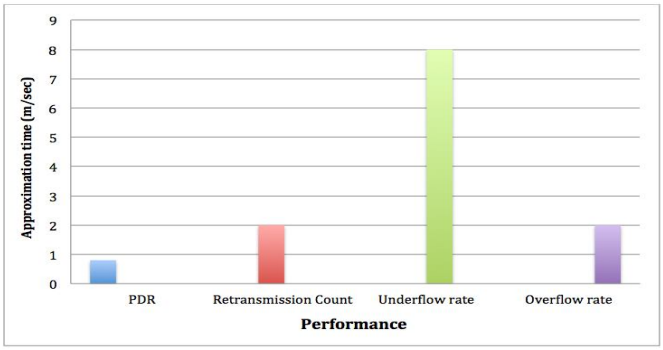

Figure: 6. Performance Analysis

In scenario I, we perform our system from 1 node to 3 nodes in which PDR, retransmission count, underflow rate and overflow rate is to be calculated which is shown in the figure 6.

3. CONCLUSIONS

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

[4] Notes in Electrical Engineering, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.

[5] T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks,"

[6] in Wireless/Mobile Security. New York: Springer-Verlag, 2008

[7] 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.

[8] 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