ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 5, May 2016

A Novel Framework for Secure Transmission in MANET

[1]Ms Raksha R. Nadgir , [2]Dr. Vandana S. Bhat
[1] M. Tech in Information Technology, ISE Department SDMCET, VTU, India,
[2] AP, ISE Department, SDMCET, VTU, India.

Abstract: ---- **In past few decades, due to defection of wired technology to the wireless era. Technology has got a revolution in the networking domain. The decentralized way in adhoc networks makes it vulnerable to attacks. If there is no centralized authority for such networks, which are not area bound then security becomes a major issue. These kind of open systems where in nodes are remotely distributed makes Mobile Adhoc NETwork most prone to attacks so security is very much needed for this technology. This paper proposes a technique which uses key management and trust based system to make MANET secure. This model focuses on providing security to network as well as information without compromising on its performance**

***Keyword*--Mobile Adhoc NETwork (MANET), Elliptic Curve Cryptography (ECC)**

I. INTRODUCTION

With the various features like quality and quantifiability, wireless networking is booming with its advanced inventions, because of these fiercely booming technologies and economical rates this has become affordable , due to which these have become more popular. Because of constant inventions in wireless networks the popularity of wireless network is more when compared to wired network in recent years.

MANET is a part of wireless networks, if MANET is formally introduced it can be said that these are the set of nodes which are mobile in nature. These nodes communicate with each other with the help of wireless links which are two ways links. This allows communication between two different parties without compromising on the quality, but any how these have their own limitation such as the transmitter issues. It is to say that when two transmitters are near enough then it is very easy for them to communicate but if they are out of range with each other, and then it becomes almost impossible to establish communications so it is held back. MANET has a solution to this drawback by using intermediate nodes to communicate; they facilitate connection between two nodes which are out of range for each other. These give permission to intermediate parties to relay the information. As we see here MANET has two types, where information is transmitted, Single hop transmission through the network and multi-hope transmission through the network [13]. In the first described way of transmission nodes which have similar radio frequencies directly communicate with each other. In multihop transmission, if two nodes i.e. source node and destination node are out of range for each other then the intervening nodes participate to help communication between source and Destination as explained. On the contrary for a simple wireless network infrastructure MANET enhances it to a suburbanized infrastructure. MANET does not have any fixed set of rules to build its infrastructure so all the nodes in the network are all engaged to move themselves arbitrarily. MANET has the capacity to make self-configuring and self maintaining network without having any assistance from the centralized infrastructure which is a main criteria in war field. The token configuration associate, when in urgent preparation to create MANET should be utilized in emergence circumstance where an infrastructure is not available, and there are no cooperative nodes in the network. Hence MANET is nothing but a distributed design which has dynamic topology, because of these features a centralized technique for observing isn’t possible anymore It is very decisive to detect the intruders and building an system to monitor and detect these intruders to make security for the network. This entire paper has been divided into four parts, the 2nd part is a discourse of related work, 3rd part is deliberation of proposed model, 4th part is all about the implementation 5th part is the discussion of results and 6th part is the final conclusion and future work .

II. RELATED WORK

Intrusion detection is nothing but a technique to find out the various activities that attempts to gather the uprightness of the resources. Since MANET is highly prone to attacks the main function of IDS is to find the disoperation of networks by watching the traffic in a network which is mobile. In intrusion detection system there is two main important models First is based on the signature method and the other is based on the anomaly. In signature based intrusion recognition system it identifies various activities in the network and tries to check it with the known. One drawback with this is it cannot detect threats which are new and unknown. On the contrary the general behaviour in systems is compared with the actual functioning to spot the difference; it is usually done with automated systems. In training phase the anomaly-based intrusion detection investigates the general activity which is always usually different from the expected then it is termed as suspicious, this can detect the various unknown attacks it is also noted that there is high negative positives for wired network infrastructure. If the statistical approach is opted the problem becomes worse due to unpredictable topology changes because of node mobility. The new way is specification based approach which serves to be ideal for any new environment; we can say that MANET is one of them. If a system takes specification as criteria for detection of the right method in the noncritical system with security specifications and then comparing it with the behaviour of object intrusions, which again makes object to act in wrong manner, these we could find out without even having exact knowledge about the nature of intrusions. These days specification based approach [14] is widely used for most privileged program, various applications and several network are present. For a adhoc network many key management schemes has been proposed. Basically, this technique is used to find efficient and useful key management for safe data transmission.

There were many intrusion detection system. that came to provide network security like watchdog was introduced [6], it was efficient IDS improving the output even in the presence of the corrupted nodes, which sent information to the next node, by receiving the acknowledgement it confirmed that the communication was secure, though it was secure the system lacked in performance it was more time consuming ,sending information to one node and then acknowledging it and again sending the data to next node was making the transmission speed low .watchdog does nothing but, it finds out the malicious node watching over the transmission of the next hop, if it finds out that the transmission to the next hop is taking more time then predefined then failure flag is raised after this path-rater comes into picture with the routing protocols to prevent the attacker node in further transmissions. The drawback in this system was, when partial dropping use to happen it use to report as failure and false report was generated ,power consumption was more . Next which came into the picture was TWO-AAC, this was introduced to solve the problems of power consumptions and partial dropping issues [8]. This finds the malicious paths by transmitting the data to three successive nodes between the source and destination. Once the data is recovered the nodes have to send the acknowledgement back with two hops distance, back to where it started. Though this handles drawback of watchdog such as receiver collision and limited transmission power, but the acknowledgement system increases the overhead of the network which in turn will reduce the life of the whole system due to battery problem in MANET

To recover the drawback of TWO-ACK there came the adaptive ACK [6] this was end to end intrusion detection system though this reduced the overhead on network but at the same time the acknowledgement received was not accurate, there were chances that acknowledgement sent could not be bona fide or genuine hence again it wasn’t that secure enough system. Adhoc is nothing but wireless connection of nodes at same peer which was made without any centralized mode. Ad hoc network always had some key issues and challenges like link level security in which there was absence of safety mechanism such as firewall. Other problem was is secure routing. In this, a protocol is generated, which is very hard to achieve. Key management is another such issue for securing the ad hoc network and is a prime requirement in case of security. Dynamic mobility is one such major problem because in ad hoc network, nodes are mobile as we know, which becomes very difficult for researchers to solve key management.

A powerful tool in achieving security is cryptography. Some methods such as symmetric way of managing key and a symmetric way of managing key was, like key distribution key storage updating keys. Revocation deleting and arching. Symmetric key management uses same key for sender and receiver for encrypting as well as decrypting and is used for long messages. Distribute key pre distribution schemes (DKPS) has 3 phases, (DKS) SSD

AND KEPT. PIKE uses sensor mode to establish the shared key. It provides good security services and scalability INF is key infection in which nodes act as trust component. Key management can also be done as a group by assigning one key for a single group [12] , and has three categories centralized distributed and decentralized simple and efficient group key management. (SEGK) is directly proportional to computing the cast and in this any node can leave or join at any time. Key server generates private group signature key which is unique and can be validated. Cluster based composite key management which also includes hierarchical clustering, mobile agent zone based key management scheme used in which each node is defined. PIKE scheme has security, facilities with fare scalability. DKPS is highly secured comparatively to other symmetric key management schemes. In the present system these key management techniques are not efficient and the techniques available are complex and time consuming [2].

III. PROPOSED MODEL

In the proposed model, by using the nodes secret key and by combining the trust factor of it with encrypted nodes identity we can build a strong system only if the nodes are trusted they can participate in transmission hence only trusted nodes will be authenticated and verified during the time of transmission .certificates will be generated for the trusted nodes. Basically it proposes the composite identification of the node based on the trust factor of the node which in turn improves the performance parameters. To enhance the security provided, we use the key management approach in combination with the cryptography technique. In the trusted model we have 4 participants the sender (SN), the receiver (RN), the trusted centre (TC), virtual central authority (VCA).

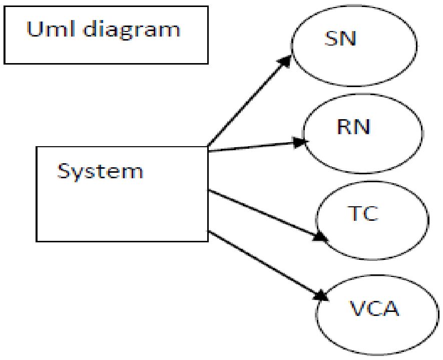

Figure 1.1: Uml diagram of the introduced system

As shown in the figure1.1, the uml diagram of the system has 4 participants these are the main components of this system just like the university the virtual authority is having all the details of each node hence when the trust centre sends the details to authority it authenticates it, each component here performs their jobs timely. In this model key management plays a main role for providing security to enhance the security, using this key management with encryption will benefit the system more. Also concentrating on the performance of the system like throughput is main goal to be attained in this system

IV. IMPLEMENTATION

Basically what happens in the process is all roaming around four components in the system, sender, receiver, trusted centre, virtual centre authority. Sender: a node sends a request for certificate to the trusted centre by registering to the network. Once it gets a certificate from the trusted centre. It logs into the network. The sender selects the file it has to send, it then sends the data and certificate to receiver node.

Receiver node: This receives the request, once it receives certificate it sends the sender node certificate VCA for verification , after receiving the response from VCA , it then receives the data if it is the trusted node if it is not trusted node it doesn’t receive any data it will be rejected . Trusted authority: Is responsible for receiving registration details from the nodes and then they send the request to VCA and again delegates back to the node. They also receive the certificate details for verification, they only send response to the node whether they are trusted or not . Virtual Central Authority: This receives the certification generation request from the trusted centre, in addition to creating the certificate this also creates a digital signature this adds up to the security of the system it is again a enhancement over the previous systems. After generating the certificate they are sent to trusted authority for delegating it to the node. Node authentication is done with at most priority the group of nodes is kept away from getting corrupted by the attack of un-trusted authority.

The data is again encrypted before sending it to the receiver only the node which is trusted can decrypt the data hence by doing this we can give security to information in addition to giving security to the network. Due to increasing threats double layer of security is important. Security should be given in such a way that is should be complex for the outsiders to invade at the same time not compromising on the performance of the system. For encryption we use the public key cryptography, here the VCA generates the public key dynamically with the certificates and the digital signature is also generated in this model. In elliptic curve cryptography they use the algebraic structures over finite fields this requires the small keys when compared to galois feilds at the same time provides equivalent security. Every date to be sent is encrypted they are converted into big integer using the public key it is dynamically generated by VCA like this cryptography in combination with node authentication make it a secure system .

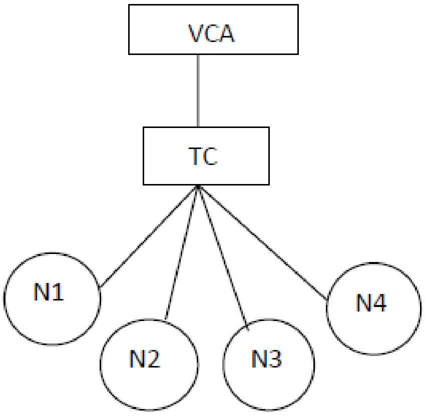

Figure 1.2 system design

As shown in figure 1.2 the VCA is above trusted authority which handles generation of certificates for the authentication. Generation of pubic key for encryption is also performed by VCA and digital signature is also generated for enhanced security. Trusted centre does the registration of different nodes these two components make sure that information and network is kept secure.

V. RESULTS

Here when we combine the techniques we should also pay due importance to the performance of the system. It has been noticed that packet delivery ratio, no of packets dropped, the throughput of the system has increased .when the packets dropped increases using the TMS we can increase the performance and the packets lost will also be taken care by the same. Here any node which is not authenticated is not allowed to even register into network hence accessing the network is not at all possible .the trusted component in the system makes it complex for the intruders to attack

VI. CONCLUSION

In this paper key management technique has been given due importance to enhance the security. Key management algorithms have been used, the cryptography technique the certificate generation method with certificate validity for secure network. Here the key pair of the node depends on the trust factor of the node for issuing the required authentication . Here using trust based method to choose the node and to authenticate it. Digital signature is also used to provide more secure environment. These all enhancements are done without compromising on the performance throughput of the network is also enhanced in this proposed model.

REFERENCES

[1] Khatri, Pallavi. "Using identity and trust with key management for achieving security in Ad hoc Networks." In *Advance Computing Conference (IACC), 2014 IEEE International*, pp. 271-275. IEEE, 2014.

[2] Chahal, Anju, Anuj Kumar, and Anuradha Rani. "SECURE KEY MANAGEMENT IN AD-HOC NETWORK: A REVIEW." *International Journal of Advances in Engineering & Technology* 7, no. 3 p: 1009.2014 july

[3] Ammayappan, Kavitha, V. N. Sastry, and Atul Negi. "Authentication and Dynamic Key Management Protocol based on certified tokens for MANETs." In *Global Mobile Congress 2009*, pp. 1-6. IEEE, 2009.

[4] Govindan, Kannan, and Prasant Mohapatra. "Trust computations and trust dynamics in mobile adhoc networks: a survey." *Communications Surveys & Tutorials, IEEE* 14, no. 2 pp: 279-298.2012

[5] Basarkod, P. I., and SunilKumar S. Manvi. "Node movement stability and congestion aware anycast routing in mobile ad hoc networks." In *Advance Computing Conference (IACC), 2014 IEEE International*, pp. 124-131. IEEE, 2014.

[6] Shakshuki, Elhadi M., Nan Kang, and Tarek R. Sheltami. "EAACK—a secure intrusion-detection system for

MANETs." *Industrial Electronics, IEEE Transactions on* 60, no. 3 pp: 1089-1098.2013.

[7] Rafsanjani, Marjan Kuchaki, Ali Movaghar, and Faroukh Koroupi. "Investigating intrusion detection systems in MANET and comparing IDSs for detecting misbehaving nodes." *World Academy of Science, Engineering and Technology* 20 pp: --------351-355.2008.

[8] Johnson, David B., and David A. Maltz. "Dynamic source routing in ad hoc wireless networks." In *Mobile computing*, pp. 153-181. Springer US, 1996.

[9] Akbani, Rehan, Turgay Korkmaz, and G. V. S. Raju. "Mobile ad-hoc networks security." In *Recent Advances in Computer Science and Information Engineering*,, Springer Berlin Heidelberg, pp. 659-666., 2012.

[10] Yang, Hao, Haiyun Luo, Fan Ye, Songwu Lu, and Lixia Zhang. "Security in mobile ad hoc networks: challenges and solutions." *Wireless Communications, IEEE* 11, no. 1 pp: 38-47,2004.

[11] Li, Wenjia, and Anupam Joshi. "Security issues in mobile ad hoc networks-a survey." *Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County* pp: 1-23,2008.

[12] El-Sayed, Ayman. "Clustering Based Group Key Management for MANET." In *Advances in Security of Information and Communication Networks*, Springer Berlin Heidelberg ,pp. 11-26., 2013.

[13] Horie, Wataru, and Yukitoshi Sanada. "Novel routing schemes based on location information for UWB ad-hoc networks." *Electronics and Communications in Japan (Part III: Fundamental Electronic Science)* 88, no. 2,pp 22-30 (2005).

[14] Pakzad, Farzaneh, and Marjan Kuchaki Rafsanjani. "Intrusion Detection Techniques for Detecting Misbehaving Nodes." *Computer and Information Science* 4, no. 1 pp. 151,2011.