IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

A Survey: Security in Patient Data Communication using Cryptographic Algorithm

Prof. Dr. R. S. Kawitkar[1], Nikita S. Karekar[2]

Professor, Dept. of Electronics, Sinhgad College of Engineering, Pune, India[1]

M.E. Student, Dept. of Electronics, Sinhgad College of Engineering, Pune, India[2]

Abstract: Wireless medical sensor networks are more vulnerable to many more attacks than the wired networks. Mobile Ad-Hoc Networks (MANETs) are particularly useful and well-suited for critical scenarios, including healthcare applications, home patient monitoring, military. MANET has number of routing protocols Ad hoc On-Demand Distance Vector (AODV) routing protocol is one of them which is the most suitable protocol for healthcare application purpose. In this project we are considering as a base protocol. Here the practical approach to prevent the inside attacks in the healthcare applications from attackers. We provide the security to the network layer by using encryption and decryption standards and a cryptographic mechanisms such as Advance Encryption Standard (AES), Rivest-Shamir-Adleman Algorithm (RSA) and Secure Hash Algorithm (SHA). Network Simulator Software (NS2) has used for the simulation purpose.

Keywords: Ad-hoc on-Demand Distance Vector, AES, RSA, SHA.

I. INTRODUCTION

In recent years we all know that the wireless sensor network (WSN) have been widely used in many day-to-day applications. The application areas of wireless sensor networks are growing rapidly. The main causes for wide growth of wireless sensor network is the cost and size of sensor devices are decreasing. The major application domains are home, office, transportation, environmental monitoring, healthcare, security and surveillance, tourism and entertainment. Wireless sensor network have been considered as one of the most important technologies that can change the future. A wireless sensor network consist of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location.

Mobile ad hoc networks (MANETs) have a security problem which receives the same problems that exist in managed, wireless networks. MANET is a mobile network which helps to connect mobile devices together by wireless link. The nodes in MANET are movable and can request to connect or disconnect the network. As a result, network topology will constantly change. In condition where mobile nodes are in the same wireless range, they can communicate directly but, if wireless is not in the same range, communication will be lost. In order to make communication available although wireless which is out of range, cooperation from other nodes is required to relay necessary messages. In networking terms it is called multi-hop network. As there is no framework or centralized management in MANET, each node has to play two roles. So that MANET node will work as a host and as a router. The router has to control and manage the routing path of each node in a multi-hop network. In order to do that, they require a standard routing protocol to facilitate the communication cooperation. Routing protocol makes MANET become attractive to network users. But MANET is also vulnerable to attack like any other networks. In fact it is more vulnerable than wired network.

MANET has various type of routing protocols and normally they are classified into proactive and reactive protocol. Ad hoc On-demand Distance Vector (AODV) protocol is reactive routing protocol. So that there is no any protection or security mechanism was built which will be able to find and give the information about the existence of spiteful attack. The black hole attack is the most common attacks for AODV routing protocol whereby nasty node will pretend to have the shortest and freshest route to destination by constructing false sequence number in routing control messages. Once the network has assumed that there is a shortest and fresh path, a Black hole node can perform various attacks such as eavesdropping, spoofing, control packet modification and denial of service.

The Ad hoc On-Demand Distance Vector (AODV) routing protocol is derived from the Destination-Sequenced Distance Vector (DSDV) routing protocol for wireless Ad hoc networks. It is a reactive routing protocol. When a node wishes to send a packet to some destination; it checks its routing table to determine if it has a current route to the destination, if Yes, forwards the packet to next hop node. If No, it initiates a route discovery process Route discovery

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

process begins with the creation of a Route Request (RREQ) packet i.e. source node creates it. The packet contains – source node's IP address, source node's current sequence number, destination IP address, destination sequence number. Packet also contains broadcast ID number Broadcast ID gets incremented each time a source node uses RREQ, Broadcast ID and source IP address form a unique identifier for the RREQ, Broadcasting is done via Flooding.

II. RELATED WORK

Karim El Defrawy and Gene Tsudik [10] present an efficient technique i.e. PRISM protocol which supports anonymous reactive routing in suspicious location based MANET's. It relies on group signatures to authenticate nodes, ensure integrity of routing messages while preventing node tracking. It works with any group signature scheme and any location-based forwarding mechanism.

Durgesh Wadbude, Vineet Raichariya [11] proposed approach uses improved of security mechanisms to introduce in the proposed techniques so that it satisfies the main security requirement and guarantees the discovery of a correct and secure route. The security mechanisms that the protocol uses are the hash chain, digital signature and Protocol Enforcement Mechanism. The performance of these two protocols (SAODV and ARAN) was tested in simulation and their communication costs were measured using the NS-2 simulator, which was suitable for the present purpose.
Pankaj Sharma and Yogendra Kumar Jain [12] has designed and studied performance of Ad-hoc On Demand Vector (AODV) protocols has been modified by including the source route accumulation feature. As low transmission power of each ad-hoc node limits its communication range, the nodes must assist and trust each other in forwarding packets from one node to another. However, this implied trust relationship can be threatened by malicious nodes that may modify or disrupt the orderly exchange of packets. Security demands that all packets be authenticated before being used.

David Cerri and Alessandro Ghioni [13] presented A-SAODV, a prototype implementation of the SAODV routing protocol. They discussed the adaptive reply decision, an experimental feature they added to their implementation to improve SAODV performance. Other possible improvements could be added.

Loay Abusalah, Ashfaq Khokhar, and Mohsen Guizani [14] has focused their work on confidentiality and integrity. Few works have been done on availability. In more recent works trust based routing in MANETs has gained some interest. Trust is playing a growing security role in an open environment where unknown devices can join or leave the system at any time. Also, due to limited processing and battery power, existing encryption based security mechanism appear too burdensome to be considered viable solutions. As defined in trust is an assessment based on experience that is shared through networks of people." These shared experiences lead to trust development that augments and decays with time and frequency of interactions. Since communication is becoming pervasive, and pervasive security is called for, it is only natural to use the notion of pervasive trust where trust relationships are ubiquitous throughout the system.

III. PROPOSED WORK

A. Scope

In the AODV routing protocol security and privacy has not been considered. (Refer fig.1 & 2).Since, this routing protocol is vulnerable to many threats. It has considered that in AODV protocol every node is truthful. Once any node declares that it has the short and fresh path towards the receiver node, other nodes may trust it. A severe attack against the routing protocols in wireless ad hoc network is denial of service attack. The node which advertises in the network responds any received RREQ by fake RREP which it said that it has fast route to the destination. But in reality when data packets are received, it simply through them out. Malicious nodes can attract all network traffics by falsely claiming to have a fresh and the shortest path to the destination. When a RREQ packet is received by a fake node, it sends back a RREP packet with a large sequence number and less hop count, which implies a fresh and shortest path to the destination. Once the source node receives the RREP packet, sends all packets to this adversary node as the next hop.

However, the nasty node drops all received packets and forms a denial of service attack against the network. To absorb high percentage of the network traffics maliciously, the position of the attacker is an important factor. If the position of an adversary node is near the transmission node or in a region where normal node density is high the ratio of packet removing by malicious node will be increased. To overcome these problems we can use SHA & AES cryptographic algorithms.

In the route request and route reply message formats are shown below. It can be seen that security field has not provided in AODV.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

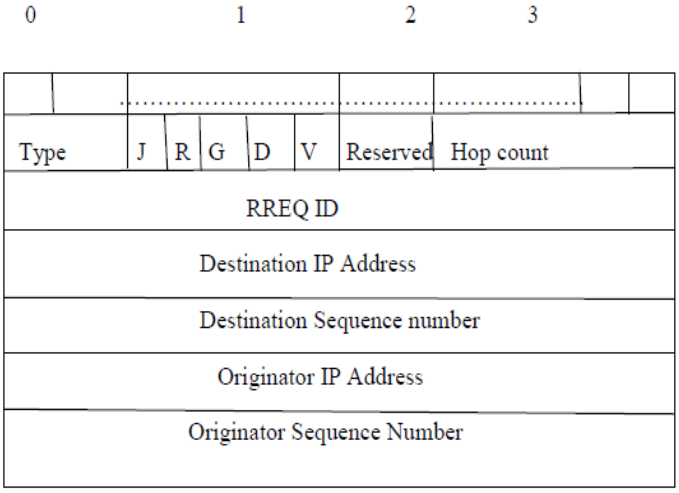

Figure 1: Route request (RREQ) Message Format

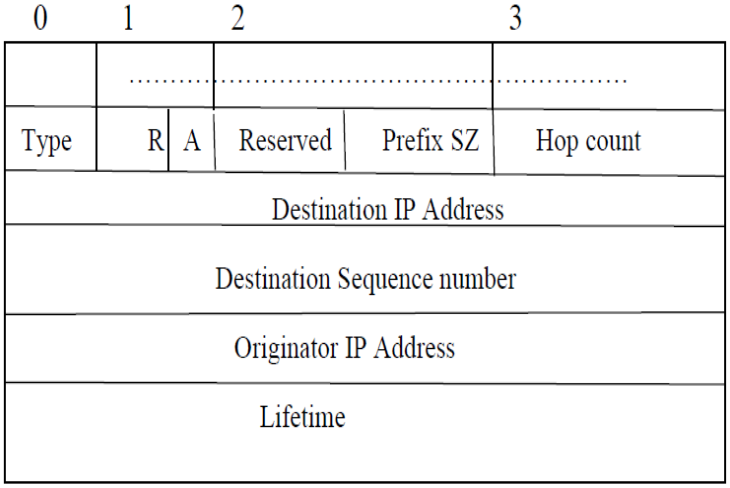

Figure 2: Route Reply (RREP) Message Format

B. Methodology:

As we know that nodes in the AODV are not secured so that some security considerations must be provided to the AODV routing protocol. The hybrid cryptography technique is used in the proposed system to provide the security between the nodes in the air. A scenario of data transmission between the two mobile nodes has been considered. Whenever a source wants to transmit the data packets to the destination, it ensures that the source is communicating with real node. The authentication service uses a key management to retrieve the extended public key, which is trusted by the third party for identification of the destination. The destination also used similar method to authenticate the source.

For the further communication confidentially a shared key is generated after execution of the key management module. In this way, all the important messages are transmitted to the destination. AES encryption of the message can be carried out in this hybrid encryption approach by using 128-bit session key value at the sender side. The hash value of message was encrypted using RSA algorithm with 1028 bit Extended Public key of the receiver. In the receiver side the decryption done for the encrypted message using AES with 128-bit session key value.

Using RSA with 1028 bit extended private key of the receiver to decrypt the encrypted hash value. To ensure the integrity the comparison is carried out between calculated and decrypted hash values. The simulation results can be seen by using network simulator. The methodology is proposed to overcome the disadvantage in the RREQ and RREP message format i.e. the security field is not provided for the AODV by providing the digital signature that is public and private key.

The Figure 3 and figure 4 explain process of Encryption & authentication and decryption & authentication.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

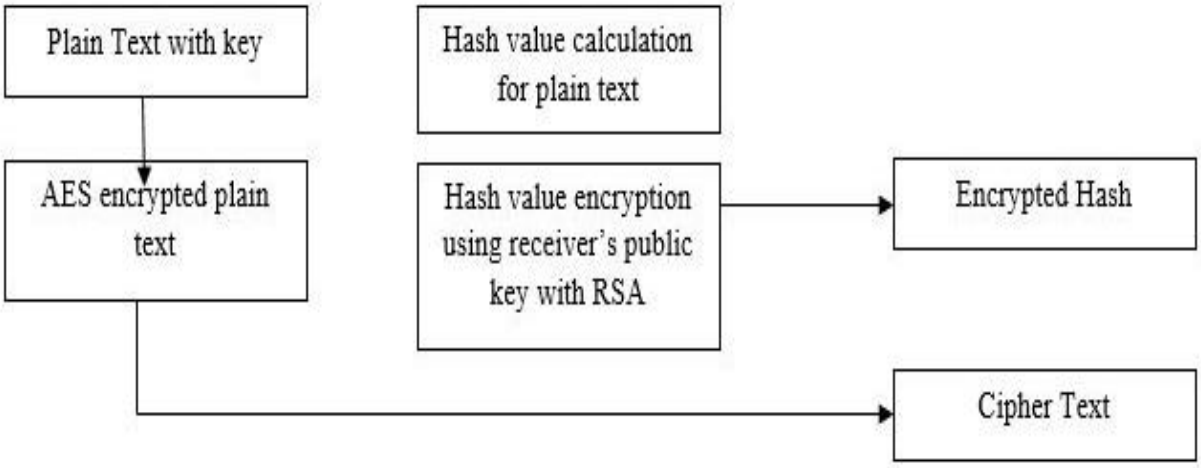

Figure 3. Encryption Process & authentication

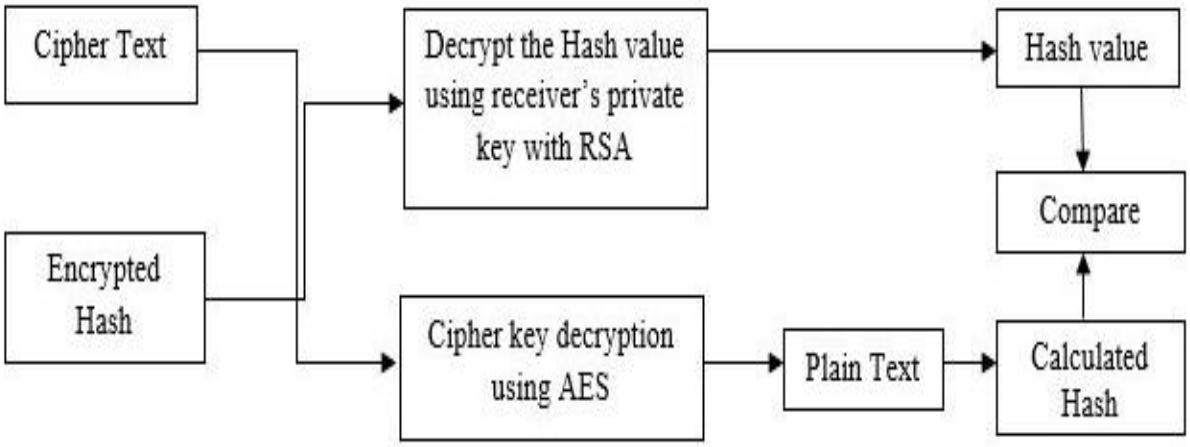

Figure 4: Decryption Process & Authentication

Following figures 5 & 6 are the frame formats for SAODV which shows extended Digital Signature fields provided for security.

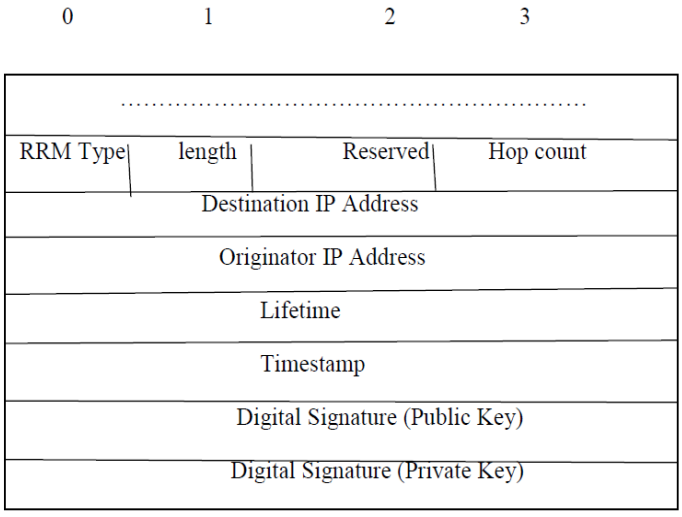

Figure 5: Route Discovery Message Format (RDM)

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

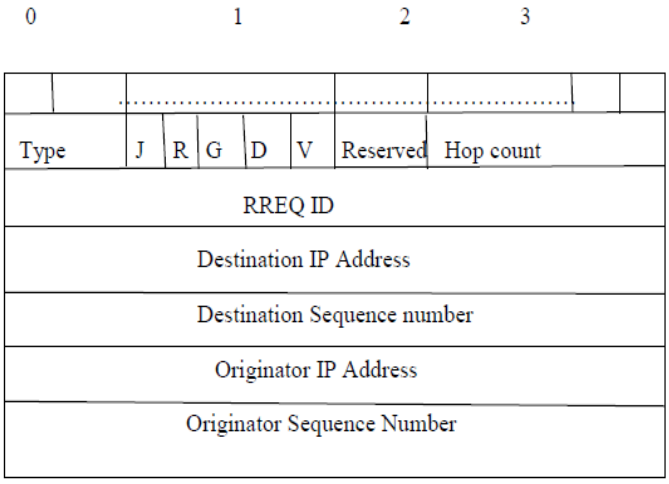

Figure 6: Route Reply Message Format (RRM)

IV. CONCLUSION

In this project the methodology will be used to provide Security for AODV. It focuses on authentication security architecture. It will provide secure data transmission between the source and destination. The proposed mechanism will authenticate the node and ensure the security of important routing information in AODV protocol. The network simulator like NS-2 software can be used to see the simulation result.

REFERENCES

[1] Xun Yi, Athman Bouguettaya, Dimitrios Georgakopoulos, Andy Song and Jan Willemson, "Privacy Protection for Wireless Medical Sensor Data", DOI 10.1109/TDSC.2015.2406699, IEEE Transactions on Dependable and Secure Computing
[2] Kamarularifin Abd Jalil, Zaid Ahmad Jamalul- Lail Ab Manan2011, "Securing Routing Table Update in AODV Routing Protocol" IEEE Conferece on Open systems (ICOS2011),SEPTEMBER 25-28,2011,Langkawi,Malasia
[3] Karim El Defrawy, Member, and Gene Tsudik, "Privacy-Preserving Location-Based On-Demand Routing in MANETs", IEEE Journal On Selected Areas In Communications, VOL. 29, NO. 10, DECEMBER 2011
[4] Durgesh Wadbude, Vineet Richariya An Efficient Secure AODV Routing Protocol in MANET, International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 4, April 2012 274
[5] Cerri and Alessandro Ghioni, Securing AODV:The A-SAODV Secure Routing Prototyped vide
[6] William Stallings, Cryptography and Network Security Principles and Practices, Fourth Edition
[7] USOR: An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks IEEE Transactions On Wireless Communications, VOL. 11, NO. 5, MAY 2012
[8] Satyendra Sing, Vinod Kumar Yadav, Ganesh Chandra, Rahul Kumar Gangwar, An Efficient and Improving The Secrity Of AODV Routing Protocol.
[9] P. Kumar and H. J. Lee. Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey. Sensors 12: 55-91, 2012.
[10] Karim El Defrawy, Member, and Gene Tsudik, Privacy-Preserving Location-Based On-Demand Routing in MANETs IEEE Journal On Selected Areas In Communications, VOL. 29, NO. 10, DECEMBER 2011
[11] Durgesh Wadbude, Vineet Richariya An Efficient Secure AODV Routing Protocol in MANET by International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 4, April 2012 274
[12] Pankaj Sharma,, Yogendra Kumar Jain Trust Based Secure AODV in MANET
[13] David Cerri and Alessandro Ghioni Securing AODV:The A-SAODV Secure Routing Prototyped
[14] Loay Abusalah, Ashfaq Khokhar, and Mohsen Guizani, A Survey of Secure Mobile Ad Hoc Routing Protocols.