AN ENERGY EFFICIENT SECURITY MECHANISM FOR MEDICAL SENSOR NETWORKS

MuthuHariharan.R.M[1],
PG Scholar, Department of IT,
SNS college of Technology, Coimbatore

muthuhariharan@gmail.com[1]

ThamaraiSelvi.K[2]
Assistant Professor, Department of IT,
SNS college of Technology, Coimbatore .

Siva.thamarai@gmail.com[2]

***Abstract*---The open nature of wireless sensor network leaves it susceptible to different kinds of attacks. It is employed in a for power efficiency wide variety of applications such as logistics, precision agriculture, telematics, medicine and healthcare etc. Wireless medical sensor networks enables healthy monitoring on users in health sites without restricting their freedom. Establishing trust is a powerful tool in improving security and performance in distributed networks such as mobile, ad hoc and sensor networks. This paper identifies the security challenges facing a Sensor network for wireless health monitoring. It protects the privacy, authenticity, and reliability of medical data with low-cost energy-efficient mechanisms. We have incorporated a two-tier authentication scheme for verifying data source and an AODV protocol with the encryption of elliptic curve cryptography**

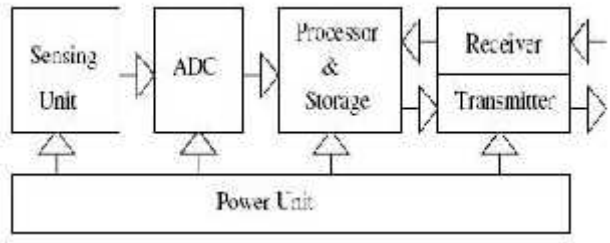
***KeywordS*-AODV, elliptic curve.**

I. INTRODUCTION

In our society, an increasing number of people have chronic medical conditions such as diabetes and heart disease. These people's health conditions could be monitored continuously and remotely, the medical experts could react to life-threatening situations such as heart attacks much more quickly. Since each patient's data is collected over a long period of time, physicians could provide more accurate diagnoses and better treatment. In Current monitoring solutions, a patient is attached to a number of medical sensors that Convey information on his or her vital signs to a bedside monitoring device. However, because these connections are wired, such a setup severely limits the mobility of the patient, which is unsuitable for long-term continuous health monitoring. Hence the wireless medical sensor network plays a vital role in the monitoring of patients.

II.MEDICAL SENSOR NETWORKS

A Medical wireless sensor network (WSN) consists of spatially distributed autonomous sensors to cooperatively monitor environmental or physical conditions such as sound, pressure, temperature vibration, motion or pollutants. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance. The medical sensors are now used in many industrial and commercial application areas which includes industrial process monitoring and control, telematics, logics precision agriculture etc.



In a network with one or more sensors .in which of each node in a sensor network is typically equipped with a radio transceiver or other a small microcontroller, wireless communication device, and an energy source which was usually a battery. The sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes similarly variable from hundreds of rupees to a few, depending on the size of the sensor network and the

complication required of individual sensor nodes. The Size and cost constraints on sensor nodes result in corresponding constraints on resources such as memory, energy, bandwidth and computational speed. A sensor network normally establishes a wireless ad-hoc network which means that each sensor supports a multi-hop routing algorithm.

III. ROUTING PROTOCOLS IN WSN

Routing protocols in the wireless sensor networks have been developed which support establishing and maintaining the multihop routes in MANET. These algorithms can be classified in to two different categories on-demand (reactive) such as DSR, AODV, and TORA and table driven (proactive) such as destination Sequenced Distance Vector protocol (DSDV).

IV. AD-HOC ON-DEMAND DISTANCE VECTOR (AODV)

AODV stands for Ad-Hoc On-Demand Distance Vector is a reactive protocol even it still uses characteristics of a proactive protocol. Adhoc On Demand distance Vector protocol takes the interesting parts in DSR and DSDV.Which was in the sense that it uses the concept of route discovery and route maintenance of DSR and the concept of sequence numbers and sending of periodic hello messages from DSDV. Routes in AODV discovered, established and sustained only when it as long as needed. To ensure the loop freedom the sequence numbers which are created and updated by each node itself, are used. These allow also the nodes to select the most recent route to a given destination node. Adhoc On Demand distance Vector protocol takes advantage of route tables. In this it stores routing information as destination and next hop addresses as well as the sequence number of a destination.

To prevent storing information and maintenance of routes that are not used anymore each route table entry has a lifetime. If during this time the route has not been used, the entry is discarded.

There are three phases
1. Route Discovery
2. Route Maintenance
3. Route Determination

Route Discovery:

In the route discovery if a node wants to communicate with another node it first checks its own routing table if an entry for this destination node exists. If the destination node doesn't exist then the source node has to initialize a route discovery.

This process is done by creating a RREQ message and also including the hop count to destination, the IP address of the source and the destination, the sequence numbers of both of them, as well as the broadcast ID of the RREQ.

This ID and the IP address of the source node together form a unique identifier for the RREQ message. At the time the RREQ is created the source node broadcasts it and sets a timer to wait for reply. The entire nodes which receive the RREQ first check by comparing the identifier of the message with identifiers of messages which are already received. If it is not the very initial time the node sees the message, it discards silently the message. When the source node receives no RREP as a response on its RREQ a new request is initialized with a higher TTL and wait value and a new ID. It retries to send a RREQ message for a predefined number of times after which, it not receiving a response and declares that the destination host is unreachable.

Route Maintenance:

When a route has been established, it is being maintained by the source node as long as the route is needed. Movements of nodes affect only the routes passing through this specific node and thus do not have global effects. If the source node moves while having an active session, and losesconnectivity with the next hop of the route, it can rebroadcast an RREQ.

Route discovery and Route Maintenance:

If though an intermediate station loses connectivity with its next hop it initiates an ROUTE_ERROR message and broadcasts it to its precursor nodes and marks the entry of the destination in the route table as invalid, by setting the distance to infinity.

Route Determination:

When the ROUTE_ERROR message is received by a neighbour it also marks its route table entry for the destination as invalid and sends again ROUTE_ERROR messages to its precursors. The node N4 moves to N4' and so node N3 cannot communicate with it anymore, connectivity is lost. N3 creates a RERR message to N2, there the route is marked invalid and unicast the message to N1.The message is unicast since we have only route passing through each node. N1 does the same thing and unicast the message to the source node. When the RERR is received at the source node and it still needs the route to the destination it reinitiates a route discovery. The new route from the source to the destination through node N5. Also if a node receives a data packet for a node which it does not have an active route to, it creates ROUTE_ERROR a message and broadcasts it as described above.

V. ELLIPTIC CURVE CRYPTOGRAPHY

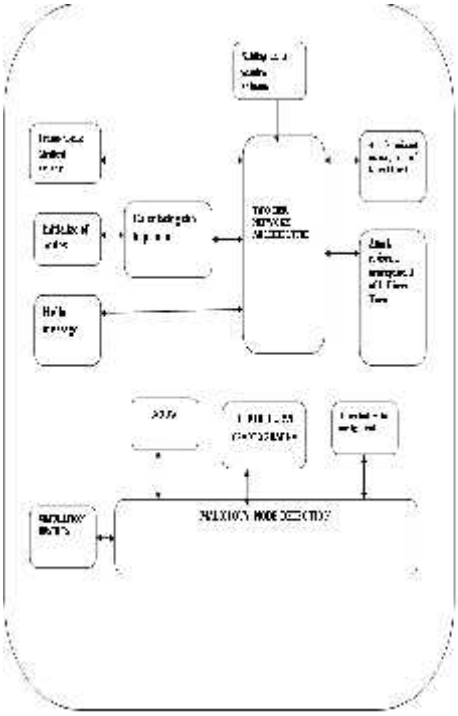
ECC offers security equalling to RSA using small key sizes. In a network when RSA uses 1024 bits of key size for the data where elliptic curve uses only 163bitsFor Key Generation ECC take 0.08 seconds were RSA take 0.16 seconds.

VI. TWO-TIER NETWORK ARCHITECTURE

The two tier architecture was designed for the medical sensor networks to provide security over the nodes. Each node was connected through intercell and intracell communication. The medical sensor network needs a two tier architecture which will be a hierarchical network. The complete network area were partitioned into collection of cells in which the cell have taken as MN's charging into SN's.

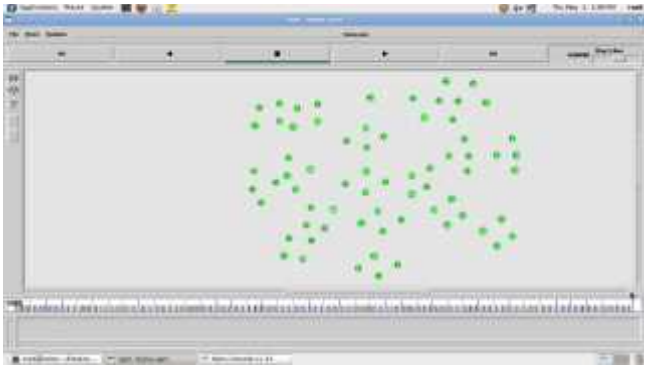
The trust management will be taken from the intercell communication and intracell communication. Here the intercell communication will be between the one cluster to another cluster and the intracell communication will be within the cluster.

VII. BLOCK DIAGRAM

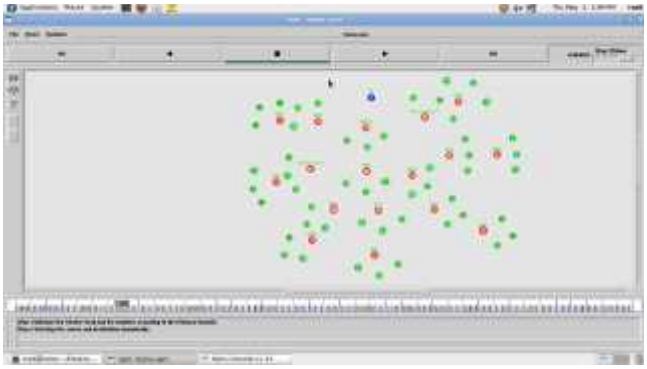


VIII. RESULTS

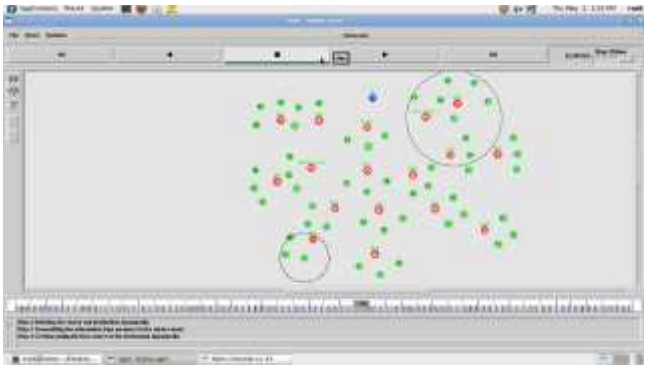
Initialization of the nodes



Selection of master nodes



Transmission of encrypted data



IX. CONCLUSION

With the emergence of widespread using medical sensor network the need of a proper trust management protocol is strongly needed. An attack-resistant and lightweight trust management scheme for MSNs has been proposed and it also have energy efficiency by using AODV routing protocols. The medical data content have been secured by encryption of elliptic curve.

X. REFERENCES

[1] "ReTrust: Attack-Resistant and Lightweight Trust Management for Medical Sensor Networks", Daojing He, Chun Chen, Sammy Chan, Jiajun Bu, and Athanasios V. Vasilakos

[2] O. G. Morchon and H. Baldus, "Efficient distributed security for wireless medical sensor networks," in *Proc. Intell. Sensors, Sensor Netw. Inf. Process. 2008*, pp., 249–254.

[3] T. Grandison and M. Sloman, "A survey of trust in internet applications," *IEEE Commun. Surveys Tuts.*, vol. 3, no. 4, pp. 2–16, Fourth Quarter 2000.

[4] D. Ingram, "An evidence based architecture for efficient, attack-resistant computational trust dissemination in peer-to-peer networks," in *Proc. iTrust 2005*, pp., 273–288.

[5] G. Theodorakopoulos and J. S. Baras, "Trust evaluation in ad-hoc networks,"in *Proc. ACM Conf. Wireless Netw. Security 2005*, pp. 1–10.

[6] R. Venkataraman,M. Pushpalatha, and T. Rao, "A generalized trust framework for mobile ad hoc networks," in *Recent Trends in Networks and Communications*, vol. 90, N. Meghanathan, S. Boumerdassi, N. Chaki, D. Nagamalai, Eds. Berlin/Heidelberg, Germany: Springer-Verlag, 2010, pp.326–335.

[7] K. Wang, M. Wu, and S. Shen, "A trust evaluation method for node cooperation in mobile ad hoc networks," in *Proc. Int. Conf. Inf. Technol. 2008*, pp., 1000–1005.

[8] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," *ACMTrans. Sensor Netw.*, vol. 4, no. 3, pp. 1–37, 2008.

[9] A. Boukerch, L. Xu, and K. EL-Khatib, "Trust-based security for wireless ad hoc and sensor networks," *Comput. Commun.*, vol. 30, no. 11–12, pp. 2413–2427, 2007.

[10] Y. Stelios, N. Papayanoulas, P. Trakadas, S. Maniatis, H. Leligou and T. Zahariadis, "A distributed energy-aware trust management system for secure routing in wireless sensor networks," in *Mobile Lightweight Wireless Systems*, vol. 13, F. Granelli, C. Skianis, Y. Xiao, and S. Redana, Eds. Berlin, Germany: Springer-Verlag, 2009, pp. 85–92.

[11] ZigBee Alliance, "Personal, home, and hospital care: technical requirements document," *Release 075111r02*, Sep. 2007.