AN Improved Energy Aware Secure Cluster Based Multiple Hop Routing Protocol for Wireless Sensor Network

V. Thilagavathi, N. Nagadeepa

Abstract*-- Due to the technological advancement in wireless communication, energy-efficient power supply, and semiconductor technology, the smart sensor becomes popular in many applications. In WSN, the private data collected and processed by the sensor node must be protected from the malicious attack. Due to the resource constraint nature of WSN, the traditional security protocols do not apply to this network as it involves huge and complex computation. Furthermore, the energy supplied by the battery is not renewable. This paper proposes a secure cluster-based multiple-hop routing protocol for prolonging the lifetime of WSN and securing the data in transit and storage. This protocol proposes the matrix transposition cryptographic techniques for securing the sensor data. This protocol compares the energy consumption and throughput of two secure routing protocols.

Keywords: Clustering, Cryptographic technique, Energy Preservation, Multi-Hop Communication, Wireless Sensor Network.

I. INTRODUCTION

Advances in microelectronic technologies have to lead to the development of cheap and portable devices that performs sensing, processing and communicating through radio transceiver. Networks of the tiny, low-cost devices deployed in a distributed environment have no fixed infrastructure, performs automated information gathering in military, industry and civil applications. WSN, using the wireless medium for communicating with the base station, provides flexibility and the network can able to work without the human intervention [1]. This network performs routing and addressing, data consolidation and data aggregation in addition to sensing the environment. Thus, the main issue in the WSN is the lifetime of the sensor due to the energy drain of the sensor, connectivity decreases and the node become dead and inaccessible.

A. ROUTING

Routing mechanism finds out a path between the source and the destination node when the device has information transmitted. In WSN, the network layer performs routing for the requested message. In multi-hop routing networks, the source node cannot transmit the data directly to a destination. Instead, the source node transmits the message through a set intermediate relay node. The intermediate node determines which neighbor node is the best node to transmit the message if the destination node is not itself [2].

B. ROUTING CHALLENGES

Due to the inherent characteristics of the sensor, routing becomes a major challenge in the wireless sensor network. The existing routing protocol designed for the wireless network does not apply to the wireless sensor network. To design a routing protocol to the wireless sensor network, we must consider a set of factors that affecting the design of the routing protocol.

Sensor node has a limited power, supplied by the batteries. When the sensor node performs computation and transmits the message through a wireless medium and exchange the information for constructing the routing table, the sensor node drains their energy very quickly. However, energy-efficient routing protocols are used to manage energy efficiently [3].

In WSN, when the number of sensor nodes used in the wireless sensor network increases, the size of the network has also increased that impacts on the overall performance of the network. Scalability of the network is the ability to accommodate the number sensor node used.

In WSN, sensor node deployed either in a random approach or in deterministic approach. In a random approach, sensor node deployed in a random area and in deterministic approach the node is deployed in predefined locations. In the random approach, the topology of the network can be changed dynamically. Initially, the sensor node is not aware of the topology used. Then it will get the topology information from the router. Dynamically changing nature of topology will affect the performance of the router.

Energy-efficient routing protocol enhances the residual energy and maximizes the lifetime of the wireless sensor network by reducing the traveling distance of data packets using the optimal shortest route. Furthermore, these protocols switch off the radio transceiver of the sensor node when the sensor node is not in use because these nodes are self-configure in nature [4].

C. HOMOGENOUS SENSOR NETWORKS

A homogenous wireless sensor network consists of a huge number of sensor nodes with equal computational power, storage, and residual energy and base station.

Revised Manuscript Received on October 15, 2019.

V.Thilagavathi, Department of Computer Science, Bharathiyar University, Coimbatore, Tamil Nadu, India. thilagavathi.research@gmail.com

Dr. N.Nagadeepa, Principal, Karur Vellalar College of Arts and Science for Women, Karur, Tamil Nadu, India, nagadeepa1012@gmail.com.

This network uses two types of network structure for data dissemination: flat and hierarchical. In flat-based routing, data-centric routing is used to aggregate the data. When the base station needs the data, it sends the query message to sensor nodes through flooding.

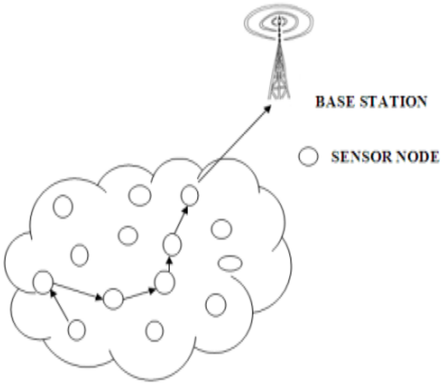

Fig 1. Flat routing

The sensor node which is having the data matched with the query message prepares the response message and sends it to a base station. The sensor node communicates with the base station through a set of relay sensor nodes. In this network, sensor nodes are stationary [5]. In a hierarchical network, the sensor nodes are partitioned into more than one group called cluster where every cluster has set sensor nodes as cluster members and a cluster head. The cluster member transmits the data to the base station through a cluster head. The transmission capacity of the cluster head is same the other sensor nodes. The cluster head performs the data aggregation and reduces the number of data transmission.

D. HETEROGENEOUS SENSOR NETWORKS

The heterogeneous wireless sensor network consists of sensor nodes and a base station. The sensor node has advanced embedded processing and communication facilities for aggregating and communicating the data with a base station. These sensor nodes are distributed densely and the distance between the nodes are not equal. When the distance between the nodes is very long, then communication of data needs more energy [5]

E. CLUSTERING

Clustering technique is preferable in hierarchical networking structure to reduce the residual energy usage and improving the overall performance of the WSN. This technique groups the sensor nodes and forms a cluster around the cluster head which performs inter-cluster connectivity and the state maintenance. In multi-hop wireless routing protocols, clustering technique forms a cluster to minimize the routing overhead, allocate the resources efficiently, perform energy management and fault-tolerant routing and to improve the throughput [3].

In clustering without the cluster head, proactive routing is preferred for intra-cluster routing whereas a reactive routing is preferred for inter-cluster communication. This type of cluster faces heavy traffic overhead when the size of the network is increased. Even though the cluster head does not have an additional hardware facility, it performs an additional function: data aggregation and consolidation, central administration of cluster. The main aim of the node clustering technique is to form a set of clusters that covers the complete set of node population used in WSN [4].

F. SECURITY IN WSN

Generally, wireless sensor network functions in a remote and inaccessible area where the maintenance of the sensor node is difficult by human beings. Therefore, WSN becomes the easy target for the attacker for lancing various attacks like physical attack, tampering, node cloning, unauthorized access. Furthermore, sensor nodes are resource constraint in nature. For that reason, it very difficult to distinguish the security breaches from a variation on link qualities, node failure. Thus, resource constraints nature of WSN needs the implementation of various security mechanisms for the secure transmission of information sensed by the sensor node [7].

Computer security is the set of policies, services and set of mechanisms that protect the computer system, network, and information from the unauthorized user. The security mechanisms ensure confidentially, availability and integrity.

Confidentiality is the security mechanism, which assures that only the authorized user accesses the confidential information and prevents the unauthorized access of information. For example, the unauthorized user does not allow accessing the credit card number, user name, and password. Data integrity maintains data accuracy and consistency. Maintenance of the data integrity ensures that message in transit, storage cannot be altered or modified by the intruder, and the data remain the same in their entire lifetime. Data availability ensures that system data and its application continue to be available at any time without any interruption. Data availability can achieve through data redundancy [8].

The traditional security protocols do not apply to the wireless sensor network because the traditional security protocols involve heavy and complex computations, which needs a high-speed processor and large storage capacity. Sensor nodes are resource-constrained in storage and processing speed. For example, the sensor node TelosB has 10 kb ram and 48 kb flash memory. Before the development security mechanism, the objective of the security mechanism must be described to protect the information and networking resources from ac tive, passive attacks and denial of service attack [1].

The active attack steals valuable information and misuses both the information and wireless sensor network. Due to the active attacks, there is heavy damage to the valuable information and the sensor network. The active attacks are a major threat to data integrity and availability. The passive attack intercepts valuable information during the transformation and does not disturb the normal work of WSN. This passive attack violates confidentiality.

The prevention of these attacks needs the implementation of authentication, confidentiality, and integrity. The design of routing protocol must implement the security services to protect the information from the attacker.

II. RELATED WORK

Due to the technological advancement in wireless communication, energy-efficient power supply, and semiconductor technology, the smart sensor becomes popular in many applications. These smart sensors sensing the physical environmental data, process and route this processed information to a base station through single-hop or multi-hop network [1][2].

The wireless sensor network is applied in many real-time applications. For example, WSN is used in a military application where the sensor detects the enemy troop movement, chemical, and biological weapons, monitoring industrial processing.

Wireless sensors are deployed in the remote and unattended area to measure the physical characteristic of the environment such as humidity, temperature, pressure, moisture, etc. Due to the resource-constrained nature and working at the area where human survival is difficult, the set of characteristics of the sensor node should be considered. The major characteristics of WSN are listed below [7].

The main research challenge in the design of WSN is that it needs energy-efficient hardware and software protocols. The processor capabilities of doing computation determine energy consumption. To save energy, the sensor node should be kept in three states: sleep, active and idle. Energy-efficient routing protocol enhances the residual energy and maximizes the lifetime of the wireless sensor network by reducing the traveling distance of data packets using the optimal shortest route. Furthermore, these protocols switch off the radio transceiver of the sensor node when the sensor node is not in use because these nodes are self-configure in nature [9].

In the hierarchical network, the sensor nodes are partitioned into more than one group called cluster where every cluster has set sensor nodes as cluster members and a cluster head. The cluster member transmits the data to the base station through a cluster head. The transmission capacity of the cluster head is same the other sensor nodes. The cluster head performs the data aggregation and reduces the number of data transmission.

WSN deployed and operated in a remote and inaccessible area and it is open to public access. Once deployed, it is very difficult to monitor the wireless sensor network. Therefore, the intruder cal easily launches various attacks [10].

In WSN, data packets transmitted over the network becomes corrupt due to routing failure, collision and channel error and the sensor node is unable to distinguish the erroneous data and the falsified data injection by the intruder. The sensitive data collected by the sensor node cannot access by the unauthorized user. Besides, the information about the sensor node such as node's Id, location and the key used for the encryption should be protected from the eavesdropper.

III. PROPOSED WORK

The major constraint of the WSN is that the sensor node operates with the energy supplied by the batteries and these batteries are not renewable. This energy is used for doing various functions: sensing, processing, continuous listening of the wireless medium and communicating the processed information with other sensor node or a base station. Due to these functions, the energy supplied by the batteries drained out and the sensor node becomes dead.

To improve the lifetime and secure the data packets transmitted over the WSN, this paper proposes a secure cluster-based energy-efficient routing protocol. This protocol uses a graph-based multiple hop routing forms the source node to a base station. This energy-efficient routing protocol enhances the residual energy and maximizes the lifetime of the wireless sensor network by reducing the traveling distance of data packets using cluster-based multi-hop communication and optimal shortest route using AODV routing. This protocol forms the cluster based on the residual energy, signal strength, and density of sensors deployed.

In this protocol, the source node initiates the route discovery function when this node needs to transmit the data. This secure routing protocol is scalable, where any number of sensor nodes can be added dynamically, and fault-tolerant in nature. This protocol also maintains survivability and ensures connectivity. To secure the data, this protocol implements matrix transposition based encryption and XOR operation using a random pairwise key.

IV. RESULTS AND ANALYSIS

This section provides a comparative analysis of AODV-MT and DSDV-MT based on the residual energy and throughput. This proposed AODE-MT protocol has implemented using NS2 2.3. In the simulation process, 50 sensor nodes deployed uniformly. Throughput means that the amount of data transmitted successfully per unit of time, measured in terms of bits or bytes/second. Some of the factors that affect throughput are a collision, channel utilization, and latency. The following graph compares the throughput (kbps) versus simulated time (ms) of both AODV-MT and DSDV-MT. This comparison shows that AODV-MT provides better performance than DSDV-MT.

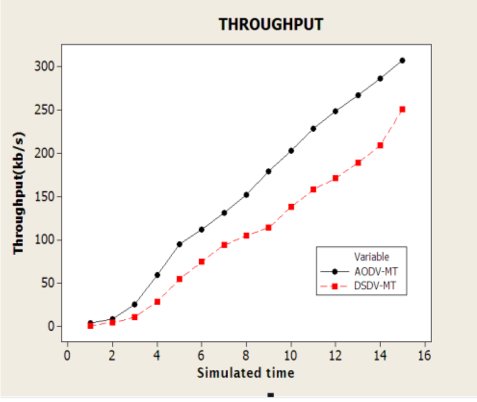

Fig 2. Throughput

The following graph compares the residual energy (j) versus simulated time (ms) of both AODV-MT and DSDV-MT. This comparison shows that AODV-MT provides better performance than DSDV-MT.

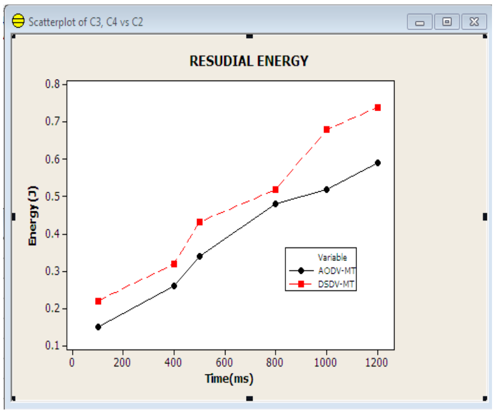

Fig.3. Residual energy

V. CONCLUSION

This paper presents an AODV-MT protocol to preserve the energy usage of sensor nodes and to secure the data transmitted using the cluster-based multiple hop communication. Further, this reliable, scalable and securable protocol ensures the confidentiality, authenticity, and integrity using the advanced encryption technique with XOR operation. This paper observes that AODV-MT is more efficient than DSDV in terms of residual energy and throughput.

REFERENCES

1. I. F. Akyildiz and I. H. Kasimoglu, "Wireless sensor and actor networks: research Challenges," Ad Hoc Networks, vol. 2, no. 4, pp. 351-367, 2004.
2. H. Nakayama, N. Ansari, A. Jamalipour, Y. Nemoto, and N. Kato, " Fault - resilient Sensing in wireless sensor networks", Computer Communications, vol. 30, no. 11, Sept. 2007, pp. 2375 – 2384.
3. J. Al - Karaki and A. Kamal," Routing techniques in wireless sensor networks: A Survey "IEEE Wireless Communications Magazine, vol. 11, no. 6, Dec. 2004, pp. 6 – 28.
4. I. Chatzigiannakis, A. Kinalis, and S. Nikoletseas, " Sink mobility protocols for data collection in wireless sensor networks", In Proceeding of the 4th ACM Workshop on Mobility Management and Wireless Access (MobiWac ' 06), Los Angeles, CA, Oct. 2006, pp. 52 – 59.
5. V. Mhatre and C. Rosenberg, " Homogeneous vs heterogeneous clustered sensor networks: A comparative study", in Proceeding of IEEE ICC ' 04, vol. 6, Paris, France, June 2004, pp. 3646 – 3651.
6. W. Ye and J. Heidemann, "Medium access control in wireless sensor networks", Technical Report ISI - TR - 580, USC/Information Sciences Institute, Oct. 2003, pp. 1 –
7. S. Khan, N. Mast, K. K. Loo, and A. Salahuddin, "Passive security threats and Consequences in IEEE 802.11 wireless mesh networks," International Journal of Digital Content Technology and Its Application, vol. 2, no. 3, pp. 4–8, 2008.
8. M. Healy, T. Newe, and E. Lewis, "Security for wireless sensor networks: a review," in Proceedings of IEEE Sensors Applications Symposium (SAS '09), pp. 80–85, New Orleans, La, USA, February 2009. [43] C. Gupta, K. Gupta, and V. Gupta, "Security threats in sensor
9. Dai, S, Jing, X, and Li, L, "Research and analysis on routing protocols for wireless sensor Networks", Proc. International Conference on Communications, Circuits, and Systems, Volume 1, 27-30 May 2005, pp. 407-411.
10. K. Akkaya, M. Younis, A survey on routing protocols for wireless sensor networks, Ad Hoc Networks 3(3) (2005) 325-349.

AUTHORS FROFILE

V.Thilagavathi, received the M.Sc in Computer Science degree from the Manonmanium Sundaranar University, Tirunelveli, Tamil Nadu in 1994 and M.Phil(CS) from Periyar University, Selam in 2007. Her research includes Network Security field.

Dr.N.Nagadeepa, is the Research Supervisor at the Bharathiyar University, Coimbatore, Tamil Nadu. She received M.C.A from Periyar University, Salem, and the P.hD in Computer Science from Mother Teresa University, Kodikanal, Tamil Nadu.