Journal of Engineering Sciences
Vol 11, Issue 3, March/2020
ISSN NO:0377-9254

Reliable Energy-Aware Routing Protocol (REARP) in Secure Routing Protocols for Wireless Sensor Networks

S.Boopathi[1], Dr.A.Senthilkumar[2]
[1] Guest Lecturer, Dept. of Computer Science, Government Arts College for Women, Nilakottai, Dindigul, Tamilnadu, India.
Mob. No: 9865812119, sbp.boopathi@gmail.com
[2] Assistant Professor, Dept.of Computer Science, Arignar Anna Govt. Arts College, Namakkal-637002. senthilkumarmca76@gmail.com

ABSTRACT

Wireless Sensor Networks (WSNs) is fastest growing technology which extensively adopting for various application services including; weather monitoring, traffic prediction, surveillance, research and academic fields etc. As the sensor nodes are randomly deployed in wireless environment, security metrics becomes most promising challenge where communication wirelesses networks. To ensure the reliability of message transmission, a hop-by-hop retransmission acknowledgement mechanism is introduced in the RER. Second, we design a metric called Reliable Energy Cost Based on Distance (RECBD) to aid RER, which is determined by analyzing the distance between the current node and the relay node, the distance between the relay node and the sink node, the current residual energy of the current node, and the link quality. The secured multipath routing protocol concentrates on security and not for reliable data transmission and energy efficient data transmission. In this paper, we focus the Energy efficient Secure Multipath Routing Protocol (EESM) protocol. The EESM protocol divided into three phases Route construction, Transfer data and Route maintenance and security. It uses Ant Colony optimization algorithm for finding the shortest path between the sensor nodes. Energy efficiency is the prime concern in Wireless Sensor Network because of the limitations on the power source for the sensor nodes. The proper routing technique can greatly contribute in energy consumption and efficient power dissipation in WSNs. Also the packet loss is major problem in the communication process.

KEYWORDS: Energy efficient Secure Multipath Routing Protocol, bandwidth, wireless sensor network.

1. INTRODUCTION

The sensor node senses the data and it is used for monitoring, tracking, detecting, collecting or reporting. The collected data transfer using wireless sensor network (WSN). Wireless sensor network connects the sensor node using wireless network. The wireless senor network components have sensor node which deployed in a hostile environment and has low power, bandwidth and computation, prone to failure and the network topology changes frequently [17]. It has major concerns about energy, security and routing. WSN consumes energy when the sensor senses the data, transmit the data between the sensor nodes and process the data. Sensor is used to sense and track in the military, collect the data during disaster management, finding the fire in the forest, find the defect in the manufacturing process, monitoring the temperature of the building and many.

When the sensor transmits the data, it consumes maximum energy. The sensor may authenticate the connection, validate and send back to the base station process takes lots of energy and power. The wireless sensor network uses to communicate between the sensor nodes, communicate between the base stations and other sensor nodes and base station to the sensor node for collecting the sensed data. WSNs secure and efficient routing is the essential factor to perform data transmission tasks. An efficient routing is the process of selecting appropriate route to forward the data

packets from source to destination. The entire process is carries out at network layer where nodes are responsible to collect the data from the participant nodes and forwards the data packets to sink node and turn forwards the processed data to the end user [3]. However, WSNs employs various cryptography based routing protocols to ensure the secure communication between the nodes or networks. Due to the dynamic characteristic of WSNs, these networks are more vulnerable for various malicious attacks such as; Black hole attacks, eaves-dropping attacks, Denial of Service (DoS) attacks and Distributed DoS attacks. Robust and efficient routing protocols can be utilized to mitigate this problem and prevent the network from malicious attacks.

2. APPLICATION

The medical and military solutions require more security than other solutions. The military application uses sensor data for enemy tracking and targeting and medical solutions store the individual medical related information.

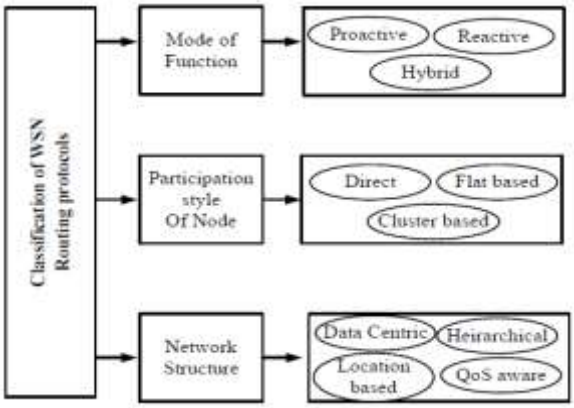

Fig.1 Classification of Routing Protocols

The most recent routing protocols ensure data confidentiality and secure routing for specific networks and resolves particular query. Therefore, the survey study suggests that the designed WSN should fulfill the end user requirements with the ability to balance the tradeoff between confidentiality, routing, communication, and energy efficiency. So, the comprehensive survey study mainly focused on prior routing protocols which provide secure communication.

3. RESEARCH GAP

There are various approaches that have been investigated in recent times associated with the security problems of WSN. It must be noted that existing system does offer some excellent security towards data as well as towards communication system in most of the cases; however, there are still some open-ended issues towards the security solution which is an alarming concern if WSN has to be a part of futuristic networking technologies. Following are certain research gap explored after reviewing existing studies.

More hypothetical and less practical approach

Existing approaches towards WSN security problems are constructed on the basis of theoretical hypothesis without considering various problems as follows:

Intrinsic problems

Implementation of security protocols demands the availability of flexible memory as well as storage sectors within a node. Unfortunately, owing to the lesser availability of storage, it is never feasible to implement high-end encryption approaches in WSN. Apart from this, the allocation of resources for executing such security protocols is very vague from the energy modeling concept in WSN. There is no standard practical energy efficient security protocol that has been proven to be resistive against practical threats in WSN.

Extrinsic problems

The selfish/vulnerable nature of node may be caused due to limited resources as well as the consequence of adversary. Apart from this, the security protocols are never studied with respect to different networking impediments like interference, scattering, fading, etc. that is very much common in any wireless network. It is also feasible for an adversary to mimic such problems in the form of threat which goes undetected to attack in core networks. At present, there is no such practical solution to this problem.

Low emphasis on grass-root problems

Every research work starts its discussion by assuming that there is an existence of some form of a specific adversary in WSN, and then the authors present their solution.

The routing helps to find the best path between the source and destination. The multipath routing protects the data in the sensor and ensures the network availability. It gives the energy efficiency and security, reliability when the data transmit in the network. The data route from base station to the sensor node (one to many), sensor nodes to a base station (many to one) and communication between the sensor nodes. The routing in WSN categorizes into three major categories flat-based, hierarchical-based and location based routing.

The sensor plays the same role in the flat based routing and does not support global addressing. . The nodes are organized into clusters and route the information through special nodes denoted as cluster heads in the hierarchical-based (sometimes called cluster-based). The cluster-based routing givens benefit of such routing algorithms is data aggregation, which saves energy and increases efficiency. The location based routing uses node location for addressing. Multipath routing techniques are considered and efficient approach to improve network capacity and resource utilization under heavy traffic conditions.

4. THE RELIABLE ENERGY-AWARE ROUTING PROTOCOL

Reliable Energy Cost Based on Distance. For nodes with different residual energies, the same energy consumption will affect them differently; that is, nodes with less residual energy should use their energy conservatively to avoid death due to exhaustion of energy, resulting in a decrease in network lifetime. Distance is another important factor affecting the energy consumption, which affects the network lifetime. Therefore, this paper defines energy cost as the RECBD metric, considering the residual energy of the nodes, the distance between the relay node and sink node, and the link quality. The goal is to minimize the energy cost of transmitting data at each time to balance the energy consumption in the network and prolong the network lifetime.

Wireless sensor network nodes or data should not capture or attacked by an attacker. Due to resource constraints WSN does not use the normal network security protocol for secure the data. The current wireless sensor protocols are designed for optimal data transmission. So, they do not consider the security. So, it might be vulnerable to attacks. It the attacker attack the routing table for disable the network data transmission, compromise the node, monitor the incoming and outgoing data. Standard cryptographic techniques protect the secrecy and authenticity of communication channels.

The information security gives the five security principal:

- Confidentiality
- Authenticity
- Integrity and
- Availability and
- Data Freshness

The Confidentiality prevents unauthorized access from an attacker. The Authenticity confirms the reliability between communication entities. The Integrity provides the mechanism for knowing whether the message tampered or not. It makes sure the message can be accessed only authorized parties. The Availability makes sure the system or service should available and should not affect by any attacks.

5. RELATED WORK

Many multipath routing protocols may not define security during the design. Wireless sensor network different with Mobile ad hoc network in many different ways. The mobile ad hoc routing technique may not be able to apply directly to the Sensor network. The sensor network nodes are static and change the topology due to node failure. Secure protocols for reliable data delivery (SPREAD) split the messages into multiple shares and deliver the message share to destination using multipath protocol. The SPREAD uses distributed N-to-1 multipath discovery protocol and more reliable and secured data collection in the wireless sensor network. The simulation shows the proposed

multipath discovery protocol is very efficient. The SPREAD does not consider the energy while transfers the data between wireless sensor nodes. The Secure Multipath Routing Protocol for Wireless Sensor Networks (SEER) proposes the scheme for energy efficient multipath routing in wireless sensor network. The SEER proposes the three phases Topology construction, data transmission and Route maintenance for secured multipath routing in wireless sensor network. It also concentrates on security a future for defending wormhole and sinkhole attacks. It assumes the data transmission for each sensor node is equal. But the sensor node may deploy in hostile environment may not take the same energy for transferring the data.

INtrusion-tolerant routing protocol for wireless SEnsor NetworkS (INSENS) secure the routing system and prevent the DOS style attacks. It does not allow the sensor node broadcast and allows only the Base station to broadcast. It uses symmetric key cryptography for confidentiality and authentication between the base station and sensor nodes due to less computational. The protocol divided in to Route discovery which includes Route request and Route Feedback, Routing Table Propagation and Forwarding Data phases. INSENS does not consider energy efficiency. The energy efficient multipath routing protocol increase the lifetime of the wireless sensor node and network. The multipath routing uses multiple path for data transmission which spread the number of nodes which saves the energy. It provides the effective load sharing to meet the Quality of service. The sink initiated proactive protocol secure Energy Efficient Node Disjoint Multipath Routing Protocol (EENDMRP) finds the multiple paths between the source and destination based on the rate of energy consumption. It uses a crypto system which uses the MD5 hash function and RSA public key algorithm. The public key distributed freely and private key distributed for each node. It has Route construction phase, Data transmission phase and transmits the data in wireless sensor network. IT do not measure energy and QoS with link reliability while transferring the data.

6. GREEDY PERIMETER STATELESS ROUTING (GPSR)

We are using Greedy Perimeter Stateless Routing (GPSR), which is an efficient and responsive routing protocol for wireless sensor networks. Unlike other routing protocols, GPSR consider the correspondence between physical position and communication in a wireless sensor network. The packet forwarding decision is made using the positions of nodes. Greedy forwarding is used to forward packets to nodes which are always gradually nearer to the destination node.

The sensor network where those greedy path are not available there will be one path need to move temporarily away from the destination node. It is recovered by forwarding in perimeter mode where a packet is transmitted consecutively closer node of a planar sub graph of full radio network connectivity graph. When it reaches to a node which is closer to the destination node it continues greedy forwarding. Another routing protocol is Dynamic Source Routing DSR, which is a self-maintaining routing technique for wireless sensor networks.

Dynamic Source Routing DSR can configure and organize the network itself independently without a human supervision. Each source determines the route to be used for delivering the data packets to required destination in DSR. In DSR there are two main phases, namely Route Discovery and Route Maintenance. Route discovery finds the optimal path between the source node and destination node for data transmission.

Route maintenance ensures the communication route remains optimal and loop-free, even if network condition changes and even it requires changing the route during transmission. The insider attacks detect and prevent the intruder within the wireless sensor network. Outside attack prevention requires to prevent from outside attacks. The passive attack does not alter the packet while transmits the data.

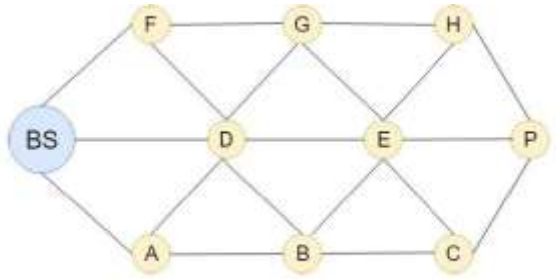

Fig.2 Node Network

This network is where the sensor nodes are uniformly deposited randomly and after distribution they become static. The sensor nodes collect the data from the field according to its sensing features and they process the data and transmit it to the base station. The sensor nodes are distributed with unique ID, a certificate signed by the base station, a unique shared key which is shared with base station.

7. ENERGY EFFICIENCY AND QOS GUARANTEE

Utilizing nodes' energy is an essential factor in designing routing protocols of WSNs to prolong the network life time of traditional WSNs. However, employing such energy-efficient routing protocols in WMSN may result in energy holes due to the large amount of data transferred in such networks. The energy-efficient path from node A to the sink node. However, over utilizing this efficient path may result in energy holes along the path. A possible solution to overcome the energy whole problem is to explore multipath techniques that satisfy both energy efficiency and QoS requirements between the node A and the sink node. Multipath routing can be interpreted in two different ways. First, it can be envisioned as a multipath exploration while employing a single path randomly at a time for data transmission. The objective of the random selection of a path is to evenly distribute the energy consumption among the explored paths. In this case, multipath routing can improve the reliability and strengthen the security by avoiding the failed or compromised paths. Second, multipath routing can also be achieved by exploring multi paths and employing them for carrying the distributed data along the explored paths simultaneously. In addition to the advantages of the first scenario, the second one will reduce the end-to-end delay and facilitate the detection and prevention of selective forwarding and sinkhole attacks.

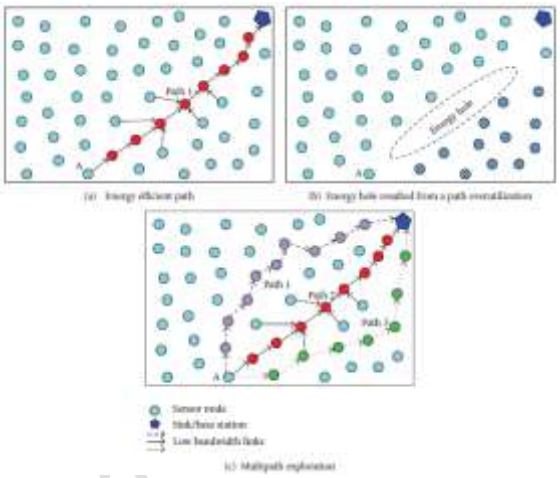

Fig. 3 Energy utilization and multipath

8. TRANSFER DATA

The data transfer uses the shortest path using Route construction phase. The base station does not assume any energy spent between the sensor nodes. The sensors placed in different climate consume different power consumption. The network knows the energy level for each bit transition. The base station sends the data request (DREQ) packet to the entire network. Once the sensor gets the data request packet, the sensor replies the data reply (DREP) packet. Find the shortest path using the previous phase. After BS finds the shortest path, the BS sends the route request message. The sensor node responds using route acknowledge message. If the key does not match, the sensor sends Error Packet (ERRP) instead of DREP. The BS ignores that path due to the malicious node in the network. The public key cryptography Elliptic curve DiffieHellman uses to validate the keys. It spends less energy for validate the key.

The node state sends DREP packets to Base station. If the Base station does not get the message in T minutes, it assumes the path affected by some attacker or malicious node available in the network. The base station chooses the different shortest path for sending the data request message to the entire network for collecting the shortest path.

9. ROUTE MAINTENANCE AND SECURITY

The BS has to calculate the energy for each path and make the decision based on the energy level. If BS uses same path, the nodes available in that path use maximum energy. The energy weight considers when the shortest path calculated from Base station. The BS changes the path when the Transfer Data phase returns some error due to public key cryptography validation or captured node in the network.

The sensor node fails due to physical environment or captured by the attackers. If the node fails, it is removed from the network and make use different path in the network. If the node fails, the sensor node updates the information through ERRP packets. The path selected from BS instead of Source or Sink node

10. CONCLUSION

We propose an efficient routing protocol, Energy efficient Secure Multipath Routing Protocol (EESM) for Wireless Sensor Networks. EESM uses multipath routing protocol which gives energy efficiency and security. The EESM do not assume energy spent for each bit transmission. It sends the data and calculates the energy for data transmission and calculates the energy based on existing collected data. The sensor may differ energy level based on location deployed (heat or cold hostile environment). The extra phase for calculating the existing data and take an average. The average energy consumption for data processing including Authentication and average energy consumption for each bit of data transmitted. SEER assumes the energy spend each node has the same value. It uses public key cryptography for authentication and authorization with pre deployed private key in sensor node.

11. FUTURE DIRECTIONS

The future vision of WSN is to embed numerous distributed devices to monitor and interact with physical world phenomena, and to exploit spatially and temporally, dense sensing and actuation capabilities of those sensing devices. Despite the fact that the execution of these conventions is promising regarding vitality proficiency, further research would be expected to address issues such as QoS posed by video and imaging sensors and real-time applications.

Future examination is to extend this security system to incorporate trust foundation and trust administration in sensor networks. The autonomous mobility management in heterogeneous networks becomes one of future research directions towards seamless mobility. Dynamically repositioning the nodes while the network is operational is necessary to further improve the performance of the network.

12. REFERENCE

1. H. Echoukairi, K. Bourgba, and M. Ouzzif. "A survey on flat routing protocols in wireless sensor networks." In Advances in Ubiquitous Networking, pp. 311-324. Springer, Singapore, 2016.

2. G. Nandini, J. Anitha, “Performance Chronicles of Multicast Routing Protocol in Wireless Sensor Network”, International Journal of Advanced Computer Science and Applications, vol. 8, no. 9, pp.284-293, 2017.

3. M. Za. Hassan, H.A-Rizzo, and F. A-Turjman. "A survey on multipath routing protocols for QoS assurances in real-time wireless multimedia sensor networks." IEEE Communications Surveys & Tutorials 19, no. 3 (2017): 1424-1456.

4. F. Ishmanov and Y. B. Zikria, "Trust mechanisms to secure routing in wireless sensor networks: current state of the research and open research issues." Journal of Sensors, 2017

5. L. Li, and D. Li. "An Energy-Balanced Routing Protocol for a Wireless Sensor Network." Journal of Sensors, 2018

6. D. Qin, S. Yang, S. Jia, Y. Zhang, J. Ma and Q. Ding, "Research on Trust Sensing Based Secure Routing Mechanism for Wireless Sensor Network," in IEEE Access, vol. 5, pp. 9599-9609, 2017.

7. M. Khalid, Z. Ullah, N. Ahmad, M. Arshad, B. Jan, Y. Cao, and A. Adnan, “A survey of routing issues and associated protocols in underwater wireless sensor networks”, Journal of Sensors, 2017

8. H. Echoukairi, K. Bourgba, and M. Ouzzif. "A survey on flat routing protocols in wireless sensor networks." In Advances in Ubiquitous Networking, pp. 311-324. Springer, Singapore, 2016.

9. A. Ghaffari and S. Babazadeh, “Multi-Path Routing Based on Network Coding in Wireless Sensor Networks,” World Applied Sciences Journal, vol. 21, no. 11, pp. 1657-1663, 2013..

10. K. Kaur and S. Waraich, "Energy Efficient Wireless Sensor Networks based on Clustering Techniques," International Journal of Computer Applications, vol. 119, no. 11, pp. 440-451, 2015.

11. P. Sharma and I. Kaur, “A Comparative Study on Energy Efficient Routing Protocols in Wireless Sensor Networks,” IJSCI International Journal of Computer Science Issues, vol. 12, no. 4, 2015.

12. Swedika Sharma, “A State of Art on Energy Efficient Multipath Routing in Wireless Sensor Networks”, International Journal of Science and Research (IJSR) ISSN: 2319-7064 Impact Factor (2018): 7.426