Energy Efficient Secure Multipath Routing Protocol For Wireless Sensor Networks

Dr. A. Senthilkumar
Professor, Department of MCA
Sengunthar Engineering College, Tamilnadu, India

Abstract

Wireless sensor network connected with small sensor for sensing the data and transfer data between source and sink. The sensor node has low computing power, bandwidth and energy. So, the traditional wired security mechanism not able to use for preventing the attacks in wireless sensor network. The multipath routing protocol uses to transfer the data in securing and reliable. Many secure multipath routing protocols are introduced for reducing the attacks in wireless sensor network. 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. This source initiated (Base Station) protocol which uses public cryptography for secure the data and introduce the protocol schema to transfer the data from sink to source.

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 sense 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 more applications. 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 [6].

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. The base station request for the data and sensor node broadcast the data in the wireless sensor network. The sensor sends the data back to Base station. The base station act as the server in the client server architecture and its broadcast, query the sensor data and routing information. The sensor act as a client and it since the data and transmit the data to base station.

2. Multipath Routing

Multipath routing increases the probability of reliable data delivery [12]. Wireless sensor routing is an important factor for saving the energy in the wireless sensor network. The routing helps to find the best path between the source and destination. The multipath routing protects the data in the sensor and ensure 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 [14]. 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 do 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.

Multipath routing transfer multiple copies of data through multipath are maintained. But only one path uses to transfer the data between source and sink. If the path fails, it uses alternative path for transmitting the data in the wireless sensor network [1]. Secure Data Collection in Wireless Sensor Networks [9] prevents compromised node (CN) and denial of service (DOS). The multipath routing may vulnerable to attacks without improve the security.

3. Secured Multipath Routing in WSN

Wireless sensor network nodes or data should not capture or attacked by an attacker. The cryptography and end -end security use for protecting the routing infrastructure. 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 (1) Confidentiality (2) Authenticity (3) Integrity and (4) Availability and (5) Data Freshness [11] [16]. 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 make sure the system or service should available and should not affected by any attacks. Data Freshness makes sure the fresh data communication between the communication entities [11]. The multipath protocol in wireless sensor network does not consider above security principal when design the protocol.

In a sensor network, when the data transfer from base station to sensor node or between senor node may attack by an attacker. Many attacks targeted to wireless sensor networks. The node capture attack which can be compromised physically capture the sensor node and extract the information from captured node [16]. The sinkhole attack tries to attract all the traffic towards the compromised node and create the sinkhole attack. The Hello flood attack sends the anonymous packets to the network. When the data send between differ node will not be able to use the network. The Denial of service (DoS) and Distributed Denial of service (DDoS) attacks send the largest number of hello packets in the network and make the entire network as busy state. The Acknowledgment Spoofing uses to attack the routing algorithm acknowledgement packets. An attacked node spoof the acknowledgment packet to neighbour node and broadcast to the entire network. The wireless sensor network security measure with a different set of metrics [17]. The security protocol considers the energy efficiency which maximizes the node and network lifetime. The security scheme flexible for cryptographic key management and fault tolerance for continuing the security service when the node failure. It should be reliable and do not lose the data while transmitting the data in the network. The sensor node may fail due to energy or other physical factor. The sensor network able to reconstruct the network topology based on the current available sensor nodes and transmit the data in the network.

Cryptography uses to prevent the unauthorized access when the data transmit in wireless sensor network. The cryptography divided into two categories Symmetric Cryptography and Asymmetric Cryptography. The Symmetric Cryptography uses the same secret key for encryption and decryption. The Asymmetric Cryptography (public key Cryptography) uses public and private keys for encrypting or decrypting the data. The cryptography requires to manage the key distribution [11]. [12] gives the key sharing protocol for Laptop Class Attacker in Wireless Sensor Network which defence against HELLO Flood Attack. Dos attack may affect the Base station and it blocks the communication between the source and sink node. The sensor will not be able to communicate with BS. The protocol [7] introduce the scheme that enables the secure site of multipath to the multiple base station in the wireless network. It also protects the location and identity of the base station. The attacker compromised node has access to internal state and cryptographic information. So, it should be turn authorized node into malicious node [8].

The security considers the key management, secure routing, and verification of sensor data. The key management help to distribute the keys between the sensor nodes and secure routing help to avoid the attacks for getting the routing information. The node captures for may inject malicious data while transfer the data in wireless sensor network. SecSens contains authenticated broadcasts, key management, routing, and reroute filtering which interact with each other component [10].

4. 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 protocol for reliable data delivery (SPREAD) split the messages into multiple shares and deliver the message share to destination using multipath protocol [5]. 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) [1] propose 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 are 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 [15]. 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 [13]. 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 transmit the data in wireless sensor network. IT do not measure energy and QoS with link reliability while transferring the data.

5. Energy efficient Secure Multipath Routing Protocol (EESM)

The security schema should avoid for inside and outside attacks, Passive and active attacks and Mote-class versus laptop-class attacks. The insider attack detect and prevent the intruder within the wireless sensor network. Outside attack prevention require to prevent from outside attacks. The passive attack does not alter the packet while transmits the data. But, the active attack alters the data or routing information while transfer the data. The mote class attack discusses about the attacker's capability equivalent to the sensor node. The Laptop class has more power and computational.

The Secure Multipath Routing with Reliable Data Transmission (SMRRD) protocol scheme based on SEER: Secure and Energy-Efficient Multipath Routing protocol [1]. The SMRRD added more secured compare than SEER and compute the energy from real time sensor average data. It considers the energy efficiency and security at the same time. The base station has the computing power and energy compare than the sensor node. The BS initiates and select the path based on the EESM protocol [1].

5.1. Overview and assumption

Static Network

All the sensor in the network placed on static network. The Mobile Ad-hoc network changes the node dynamically. The secure multipath routing applicable only for static wireless sensor networks.

Initial Energy level

The sensor node uses battery for power consumption and difficult to change or recharge. The initial energy level is constant.

Deploy node with shared key

The sensor node deployed with unique ID, a certificate (signed by BS), a unique shared key (shared with base station).

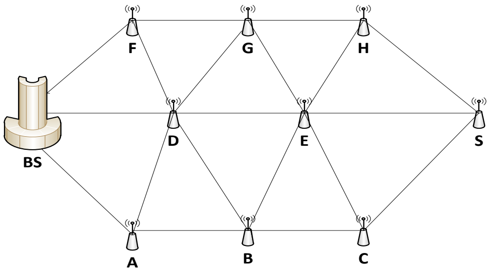

Figure 1

5.2 Route construction

Secure Multipath Routing with Reliable Data transmission is source initiated a protocol. When multiple paths use for transferring the data from source node to sink node, the order will be different. The sequence identifier added to make sure the sequence order. The BS base station initiates and send a Route Request (RREQ) packet to each sensor node in the network. The sensor node broadcasts to near sensor node for collecting the path with connected sensors. The packet broadcast to the entire network for collecting the RREQ. Now, each node has a Route Request message and update the neighbour list in the routing table. When each node gets the RREQ message, the node follows these steps.

- Current_node certificate uses authenticate neighbour node with the public key of the BS. If authentication fails, do not add in neighbour_list
- Get the previous_node address and add in the neighbour_list
- Change the previous _node to current_node
- If the Route Request available in received_message_list with Packet_sequence_number, do not rebroadcast. Otherwise, store Packet_sequence_number in received_message_list and rebroadcast the Route Request.

The RREQ packet (Figure .2) send to entire sensor network for collecting the neighbour list. After collecting neighbour list, the base station has information about all the path between from base station to sink node. The base station wait for M time to reach the Route Request message reach to sink node.

The base station sends the Route Collection (RCOL) message to the entire network. The sensor node involves in network broadcast the message to neighbour sensor. When the sensor get the RCOL message, the sensor complete the following steps.

- Base station broadcast Route Collection(RCOL) message
- Current_node certificate uses authenticate neighbour node with the public key of the BS. If authentication fails, do not add in neighbour_list
- Each node, Get the previous_node address and add in the neighbour_list
- Each node, Change the previous _node to current_node
- If the Route Request available in received_message_list with Packet_sequence_number, do not rebroadcast. Otherwise, store Packet_sequence_number in received_message_list and rebroadcast the Route Request.
- Each node broadcast entire network

When each sensor node receives the RCOL packet, it reply back to the base station through the Route Reply (RREP) packet. The RREP packet has addressed, information about the current node, the energy spent for transmission the data between the previous node and current node and list of neighbour list node. Each node store the energy spent for transmitting the data from privous_node to current_node. Finally the Base station have a list of all nodes neighbour list and energy spent to reach the sink node. The base station has all the information for build the weighted directed graph with neighbour's information.

previous_node	**current_node**	**neighbor_list**	**Packet_sequence_number**	**received_message_list**

Figure 2

The Complete weighted directed graph G = (N, E) which define the travelling salesman problem (TSP) where N is the set of nodes and E is the set of path connecting with all sensors. All the edges (i,j) € E assigned the energy Eij which is the distance between sensor node i and j Eij defined in the Euclidean space and defined in the following

$$E_{ij} = \sqrt{(xi - xj)2 + (yi - yj)2}$$

The ant colony system (ACS) a message k in the sensor r chooses the sensor s to move to among those which do not belong to its working memory Mk applying the formula

$$s = \begin{cases} \arg\max\limits_{u \notin M_k} \left\{ [\tau(r,u)] \cdot [\eta(r,u)]^{\beta} \right\} & \text{if } q \le q_0 \\ S & \text{otherwise} \end{cases}$$

where the is the amount of sensor range on edge (r,u), (r,u)i s a heuristic function which has the distance between sensor r and u, B is a parameter which energy the, q is a value chosen randomly with uniform portability in [0,1], S is the random variable selected according to the following formula

$$p_k(r,s) = \begin{cases} \dfrac{[\tau(r,s)] \cdot [\eta(r,s)]^{\beta}}{\sum\limits_{u \notin M_k} [\tau(r,u)] \cdot [\eta(r,u)]^{\beta}} & \text{if } s \notin M_k \\ 0 & \text{otherwise} \end{cases}$$

Pk(r,s) is the probability to send the message k from node r to s node. The BS first choose the shortest path and follows the next shortest path for get the packets. The base station collect the shortest paths with different parameters like energy and the distance between two nodes.

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 sensor 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 reply the data reply (DREP) packet. When the sensor get DREQ packet from BS, it follows these steps.

- Validate the message with a unique shared key. If the key matches, accept the packet. The unique shared key uses for communicate with base station with entire lifecycle.
- If the current_node is destination node, do not rebroadcast.
- If the current _node is not destination node, rebroadcast the message based on neighbour_list

Finally the base station collects all the data reply and 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 Diffie–Hellman 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.

6. 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 consider when the shortest path calculated from Base station. The BS change 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

7. Conclusion.

In this paper, 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 [1]. It sends the data and calculates the energy for data transmission and calculate 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 [1] 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.

10. References

[1] Nidal Nasser and Yunfeng Chen, Secure Multipath Routing Protocol for Wireless Sensor Networks, 27th International Conference on Distributed Computing Systems Workshops (ICDCSW'07), 2007, IEEE

[2] Wenjing Lou, an Efficient N-to-1 Multipath Routing Protocol in Wireless Sensor Networks, IEEE, 2005

[3] Marco Dorigo, Ant colonies for the traveling salesman problem, TR/IRIDIA/1996-3

[4] Arvinderpal S, Nils, Hans, Vipul, Sheueline, Energy Analysis of Public Key Cryptography for wireless sensor network, IEEE

[5] Lou, W.; Kwon, Y. H-SPREAD: A Hybrid Multipath Scheme for Secure and Reliable Data
Collection in Wireless Sensor Networks. IEEE Trans. Veh Tech. 2006, 55, 1320–1330.

[6] Yan-Xiao Li,Lian-Qin, Qian-Liang, "Research On Wireless Sensor Network Security, 2010 International Conference on Computational Intelligence and Security

[7] Jing Deng Richard Han Shivakant Mishra, “Intrusion Tolerance and Anti-Traffic Analysis Strategies For Wireless Sensor Networks”, Proceedings of the 2004 International Conference on Dependable Systems and Networks (DSN’04), 2004, IEEE

[8] Thomas Claveirole and Marcelo Dias de Amorim,Michel Abdalla, Yannis Viniotis, “Securing Wireless Sensor Networks Against Aggregator Compromises”, 2008 IEEE

[9] Tao Shu, Marwan Krunz, Sisi Liu, “ Secure Data Collection in Wireless Sensor
Networks Using Randomized Dispersive Routes” IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 9, NO. 7, JULY 2010

[10] Faruk Bagci, Theo Ungerer, Nader Bagherzadeh,"SecSens - Security Architecture forWireless Sensor Networks", 2009 Third International Conference on Sensor Technologies and Applications

[11] Ali Modirkhazeni,Norafida Ithnin#2, Othman Ibrahim#3, "Secure Multipath Routing Protocols in Wireless Sensor Networks: A Security Survey Analysis", 2010 Second International Conference on Network Applications, Protocols and Services

[12] Md. Abdul Hamid1, Md. Mamun-Or-Rashid2 and Choong Seon Hong3, "Defense against Lap-top Class Attacker in Wireless Sensor Network", Feb. 20-22, 2006 ICACT2006

[13] Shiva Murthy G, Robert John D’Souza, and Golla Varaprasad, " Digital Signature-Based Secure Node Disjoint Multipath Routing Protocol for Wireless Sensor Networks", IEEE SENSORS JOURNAL, VOL. 12, NO. 10, OCTOBER 2012

[14] Ravindra Gupta 1, Hema Dhadhal 2, " Secure Multipath routing in Wireless Sensor Networks", International Journal of Electronics and Computer Science Engineering

[15] Jing Deng, Richard Han, Shivakant Mishra, "INSENS: Intrusion-Tolerant Routing in Wireless Sensor Networks", University of Colorado, Department of Computer Science Technical Report CU-CS-939-02

[16] Dr. A. Senthilkumar, Secure Multipath routing Protocols in Wireless Sensor Network: a survey Analysis, IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), Vol. 3, No. 1, 2013

[17] T.Kavitha, D.Sridharan, " Security Vulnerabilities In Wireless Sensor Networks: A Survey", Journal of Information Assurance and Security 5 (2010) 031-044.

AUTHORS PROFILE

Dr. A.Senthilkumar received the MCA Degree from the Madras University, India, in 1999. He received the M.Phil degree in Computer Science, Manonmaniam Sundharnar University, Tirunelveli, India. He received the Ph.D degree in computer applications from Anna University, Chennai, India. He is Currently Professor in Department of MCA, Sengunthar Engineering College, Tiruchengode, Tamilnadu, India. He has 13 Years and 7 Months of Experience in Teaching. His fields of interest, Computer Networks, Network Security, Wireless Sensor Networks. He has 5 Publications in International journals to his credit. He has presented 13 papers in State, National, and International conferences.