 ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print)

A Study on Secure Routing Protocols for Wireless Sensor Networks (WSN)

[1]Ishu Gupta, [2]Dr. Harsh Sadawarti, [3]Dr. S.N. Panda
[1]Dept. of CSE, RIMT-MAEC, MGG, Punjab, India
[2]Principal & Director, RIMT-IET, MGG, Punjab, India
[3]Director Research, Chitkara University, Rajpura, Punjab, India

Abstract
Wireless Sensor Network (WSN) is a collection of randomly distributed sensor nodes which mutually recognize and gather the information within the network that dynamically self-organizes in arbitrary and temporary network topologies without relying on pre-existing fixed network infrastructure. Due to unreliable wireless media and limitation of node resources in terms of storage, communication bandwidth and range, many challenges arise in ensuring the security of sensor nodes. Many techniques have been proposed to ensure the security in wireless networking. In this paper, various secure routing protocols have been studied where main considerations are on factors like RSSI, energy consumption and also the vulnerability of the nodes.

Keywords
Routing Protocols, WSNs

I. Introduction

It has been rightly said that your network is your net worth. It is very important to collaborate and work as a team for success and growth in personal life. Similarly a computer which is not connected with other computers becomes an information island and cannot achieve the optimal computing power needed [4]. To connect with other computers the two options are to either use wires or go wireless. Installation of LAN cables is cumbersome and time consuming so only option left is to depend on the wireless media. Wireless networking offers a host of advantages but the main disadvantage is its security. It is very difficult to contain the air waves and rogue nodes can breach the security and compromise the performance [11] of wireless network. Many techniques have been projected to ensure the security in wireless networking. It is evident that for making the wireless network secure the data is broken into packets and then the route chosen is such that it takes into account the distance between the nodes, battery power, Vulnerability factor etc.

II. Routing Protocols in Wireless Sensor Networks

The sensor nodes collect audio, seismic, and other types of data and cooperate to perform a high level task in the network. Sensor nodes are severely controlled by the amount of battery power available, limiting the lifetime and quality of the network. Since wireless communications consume significant amounts of battery power, sensor nodes should spend as little energy as possible receiving and transmitting data. It is necessary for communication protocols to maximize nodes' lifetimes, reduce bandwidth consumption by using local collaboration among the nodes. In a network while communicating with each other, each sensor node has a packet to be sent to the distant base station (BS). If each node transmits its sensed data directly to base station, then power depletion occurs quickly. The LEACH protocol presented is an elegant solution to this data collection problem, where a small number of clusters are formed in a self-organized manner. A designated node in each cluster collects and fuses data from nodes in its cluster and transmits the result to the BS. LEACH uses randomization to rotate the cluster heads and achieves a factor of 8 improvement compared to the direct approach, before the first node dies.

There is also an improved protocol called PEGASIS (Power-Efficient GAthering in Sensor Information Systems), a near optimal chain-based protocol that is an improvement over LEACH. In PEGASIS, each node communicates only with a close neighbor and takes turns transmitting to the base station, thus reducing the amount of energy spent per round. This approach will distribute the energy load evenly among the sensor nodes in the network. It eliminates the overhead of dynamic cluster formation, minimizing the distance non leader-nodes must transmit, limiting the number of transmissions and receives among all nodes. Nodes take turns to transmit the fused data to the BS to balance the energy depletion in the network and preserves robustness of the network as nodes die at random locations. Simulation results show that PEGASIS performs better than LEACH by about 100 to 300% when 1%, 20%, 50%, and 100% of nodes die for different network sizes and topologies. PEGASIS shows an even further improvement as the size of the network increases [8].

In order to save the energy of the WSNs, cluster-based WSN systems are in use. There is a new cluster-based routing protocol, name Quasi-Centralized Clustering Approach (QCCA), which focuses on energy usage and vulnerability factor of a sensor node. The LEACH allows only single-hop clusters to be constructed. QCCA finds an interconnected set of clusters covering the entire node population [6]. QCCA is a sub-optimal scheme where the nodes employ the mixed communication modes: single-hop mode and multi-hop mode periodically. This mixed communication modes can better balance the energy load efficiently over WSNs. It completely eliminates redundant transmissions by ensuring, via carrier sensing (CSMA-CA), only one head sensor in each cell transmits and communicates with the sink, which can be either mobile or stationary. This approach reduces both energy consumption and communication bandwidth requirements, and prolongs the lifetime of the WSN. The simulation results indicated that this scheme provides automatic adaptation to different routes when network condition changes. Also, it is robust for unpredictable link failures. QCCA not only focus on the shortest path, but also on energy awareness and vulnerability factor of nodes.

For wireless sensor networks based on dynamic key cryptography, there is also an energy efficient secure routing like Weight Based AODV protocol for the routing process in which the weight of a route is decided by four factors: the speed of nodes, the power level of battery and the Bandwidth. It is based on vector group, by which it is able to establish the pair wise keys independently to provide security to the network [10]. The sensor nodes are organized into clusters and a cluster head is elected within each cluster. Communication between sensor and the sink takes place at the three levels: sensor→c1uster-head→sink. Simulation results show that the proposed scheme could reduce the communication overhead from o (2N) to o (N). This method provides a better security performance with a low memory overhead, high

Throughput, minimum number of hops for routing and less amount of Energy consumption.

There are various performance metrics usually considered with WSN are power consumption, connectivity, scalability, and limited resources. Malfunctioning of a few sensor nodes, due to hardware or lack of energy in the network will cause greater consumption of energy and rerouting of packets [3]. Triple Umpiring System (TUS) has already been proved its better performance on mobile ad hoc network (MANET) in which each node in the path from source to destination has dual roles to perform: Packet forwarding and umpiring. The modification of TUS for Wireless Sensor Networks provides security for routing and data forwarding operations by incorporating mine detection. There is comparison of ESRP-M (ESRP using Mine detection) with MMDP (Multipath secure routing protocol for flat network). Using Qualnet 5.0 simulator, simulation results show that Mine detection significantly improves the Packet Delivery Ratio and the latency in packet delivery.

In WSNs, the existing multipath routing schemes have confirmed the effectiveness of traffic distribution over multipaths to fulfill the quality of service requirements of applications. However, the failure of links might significantly affect the transmission performance, scalability, reliability, and security of WSNs [1]. Thus, it is desirable to design a reliable and service-driven routing scheme to provide efficient and failure-tolerant routing scheme. A routing protocol based on AODV, namely, service-oriented multipath AODV (shortly as SM-AODV), which includes the following features.

1. By considering the security of data delivery, an adaptive load-balancing multipath routing scheme to enhance the data confidentiality in the service-oriented WSNs. The difference is that it uses the secret sharing algorithm to separate the data packets according to the proposed path vacant ratio.
2. The path vacant ratio can be used to evaluate the load over multipath, which is derived from taking account of load balancing, path load, important paths, and importance of nodes over multipaths.
3. An adaptive congestion control scheme is proposed to adaptively adjust packet delivery rate over each path according to the congestion level that maintained the HELLO message.

This design is expected to provide effective routing performance for multipath and enable WSNs to provide reliable application-level services.

In order to ensure data security and quality of service required by an application in an energy efficient way, there is a mechanism for QoS routing with coding and selective encryption scheme for WSNs. In the proposed protocol, RS coding is used to provide reliability and security. The sink node decides on the paths selection process in order to satisfy the reliability or the delay requirements by an application and the number of these paths is determined to enhance the reliability. Using these techniques, attacks such as the sinkhole and wormhole are no longer related. The encrypted fragments from the same RS codeword are transmitted through different disjoint paths. The per hop packet transmission strategy improves the reliability of each path and increases the probability of successful packet delivery to the sink.

A security routing algorithm W-GEAR (Work-based GEAR,) based on node work reputation evaluation is proposed to improve the security performance of GEAR (Geographical and Energy Aware Routing) [7]. "Work" is introduced in W-GEAR routing algorithm, Sink recognition mechanism is used to record real time forward data, comprehensively consider the distance factor between nodes, give the nodes comprehensive reputation evaluation value, provide routing with reputation value, so as to recognize selective forward and data tampering. NS2 simulation experiments show that the W-GEAR improves the ability of identifying malicious nodes and increases the security of GEAR.

There is also an algorithm which considers a group of nodes with all the parameters defined to each node, initially energy consumed by each node is found which directly relates to the battery life of a node, some of the nodes are shown as malicious nodes which is carried out for static and dynamic network [9]. Two parameters are considered while routing, while dividing the sensor nodes into different clusters and ensured with trust and weight of each node to be in the path of routing. Each node has direct and indirect trusts values assigned, which will be used for security check of the node. This algorithm detects suspicious transmission and consequent identification of malicious nodes for disseminating the information in the network. A simulation is made to appear as a real time by making node to move continuously with change in its parameters. Simulation is done in Open source flat form using the C++ coding and results show that there is lot of reduction in the packet loss, misrouting.

Current trust-aware routing protocols using traditional cryptographic techniques are not capable of effectively tackling this serious problem. Against this, A Fuzzy Based Trust-Aware Routing Framework (FBTARF) is the proposed method for security improvisation in dynamic WSN. FBTARF provides energy-efficient routing and reliable trust using fuzzification methods. For the survival of wireless sensor network under harsh and hostile environment, FBT ARF provides trustworthiness and energy efficiency [2]. With the concept of innovative trust management, FBTARF enables a node to keep track of the trustworthiness of its neighbors and there by select a reliable route path. The dynamic nature of FBTARF is analyzed by means of detailed evaluation using simulation. Fuzzy based TARF effectively protects WSN from severe attacks through dynamic replaying routing information. Using FBTARF, Extensive simulation and empirical analysis with large scale WSN produces high resilience and scalability. The comparison analysis based on normal T ARF and Secured Fuzzy based trust aware routing framework (FBTARF) model is developed and the results show that the secured fuzzy model provides better results in terms of security, packet delivery ratio and energy conservation.

An energy efficient multipath routing protocol called mEENDMRP (modified Energy Efficient Node Disjoint Multipath Routing Protocol) which provides better energy efficiency, security and reliability authentication than AOMDV protocol [5]. mEENDMRP provides security through the use of asymmetric key cryptographic algorithm RSA and MD5 hash function. The first step in the EENDMRP is route construction. The second step is finding the node disjoint multiple paths based on the rate of energy consumption and filled queue length. The third step is secured data transmission among the multiple paths using digital signature based cryptographic system using RSA algorithm and MD5 hash function. mEENDMRP protocol is designed only to support text data routing.

III. Conclusion and Future work

Existing routing protocols are subject to a variety of attacks that can allow attackers to influence a victim's selection of routes or enable denial-of service attack. So, necessity of secure routing protocol is inevitable. For security we mainly consider the following attributes: availability, confidentiality, integrity,

authentication, authorization and non-repudiation. In designing security mechanisms, one must consider the attacks variations as well as the characteristics of the attacks that could be launched against the ad hoc networks [12]. Many attacks are only possible or only effective, if the malicious party is a participant of the network, so it is highly important to implement secure mechanisms to authenticate entities entering the network. In the proposed methodology of work, after investigating various security attacks, a secure routing solution will be provided for some particular attack against routing protocol. After that, Simulation of proposed Secure Routing model based on cooperation between nodes will be done with the help of Matlab.

Sensor networks with 100nodes will be implemented to carry out extensive simulations. The sensor field's dimension will be 0.01 Kilometer Square. Then the transmission power, receiving power and electronics power of each node will be calculated. If the txc, trx, elx power is low then the node will be simulated to die. The alive nodes will be found out and which node has high energy will become a cluster head. Then the RSSI value for each node will be computed by the following formula

RSSI=-10n log10 (d) + A

Where n is propagation exponent, d is the distance from the sender and A is the received signal strength at one meter of distance. If sender wants to send the data to receiver then both know the RSSI value i.e. the receiver and sender know the value of each other.

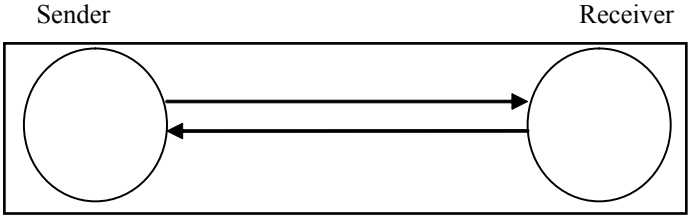

Fig. 1: Communication in Between Sender and Receiver

The problem of routing can be consider as designing a policy at each node, so that the overall path from source 'S' to destination 'D' is optimal.

$IP = \sum((1/RSSI)^2$

Where RSSI is the receiving signal strength indicator of a path as shown in above diagram, here the square value of $(RSSI)^2$ is proposed to minimize the effect of low energy node.

For example: let suppose if there are two path A and B are available from source to sink and both path have three node .the RSSI value of three node in path A are 0.9, 0.9 and 0.1 while in path B it is 0.6, 0.3 and 0.7.so if we take simply the summation of the RSSI factor of these nodes, then both paths have same RSSI cost i.e. 1.9 and protocol will chose randomly any one of it, which is not correct. The path B must be chosen as it has nodes having RSSI evenly distributed. Now if we take the square of the rssi factors of these nodes and then take summation, it gives us correct results; 1.63 for path A and 1.21 for path B. Hence, the protocol will choose path B, which is the correct decision. In our scheme, the summation of the square of impact factors of nodes is represented by RSSI.

Intuitively, a path that has high value of IP means that the path contains critical nodes. Hence, the route having low IP value produces the best energy efficient routing.

In the proposed approach, there are two phases of operation: First is setup phase and second is the steady-state phase. In the setup phase, control information is flooded in the entire network. But this flooding is different from traditional flooding. Starting from the CH, every node broadcasts the IP value to its neighbors. Whenever the nodes receive the IP values from their up tree neighbours, they store these IP values along with the corresponding node ID in their routing tables. Then these nodes select the minimum IP value from their routing tables, simply add their own IP values in it and forward it to their neighbours. This process continues till the source node.

In the steady-state phase, whenever a source node wants to send data to its CH, it chooses that neighbour from its routing table who has lowest IP value. In this way, when a node sends data to its neighbour, the receiver node sends an acknowledgement to the sender node after receiving the data. This acknowledgement also contains its updated IP value. The sender node then updates its routing table after receiving the acknowledgement from its neighbour. This process continues till the packets reach to the CH.

Then plot of number of failure v/s number of packets and number of packets v/s IP will be compared.

References

[1] Li, S.; Zhao, S.; Wang, X.; Zhang, K.; Li, L.,"Adaptive and Secure Load-Balancing Routing Protocol for Service-Oriented Wireless Sensor Networks", Systems Journal, IEEE, Vol. 99, pp. 1-10.

[2] Sakthidevi, I.; Srievidhyajanani, E.,"Secured Fuzzy Based Routing Framework for dynamic wireless sensor networks", Circuits, Power and Computing Technologies (ICCPCT), 2013 International Conference on, pp. 1041-1046, 20-21 March 2013.

[3] Subramanian, G.; Amutha, R., "Efficient and secure routing protocol for wireless sensor networks using mine detection An extension of triple umpiring system for WSN," Computing Technology and Information Management (ICCM), 2012 8th International Conference on, Vol. 1, no., pp.141,145, 24-26 April 2012.

[4] Huei-Wen Ferng; Rachmarini, D., "A secure routing protocol for wireless sensor networks with consideration of energy efficiency," Network Operations and Management Symposium (NOMS), 2012 IEEE , vol., no., pp.105,112, 16-20 April 2012.

[5] Sangeetha, R.; Yuvaraju, M., "Secure energy-aware multipath routing protocol with transmission range adjustment for wireless sensor networks," Computational Intelligence & Computing Research (ICCIC), 2012 IEEE International Conference on , vol., no., pp.1,4, 18-20 Dec. 2012.

[6] Noor M. Khan, Ihsan Ali, Zubair Khalid, Ghufran Ahmed, Rodica Ramer, Alex A. Kavokin, " Quasi centralized clustering approach for an energy-efficient and vulnerability-aware routing in wireless sensor networks." HeterSanet 2008: 67-72.

[7] Yang Song; Jian-pei Zhang; Li-Jie Li; Qing Wang, "Work-based Reputation Evaluation Secure Routing Algorithm in wireless sensor networks," Millimeter Waves (GSMM), 2012 5th Global Symposium on , vol., no., pp.490,493, 27-30 May 2012.

[8] Lindsey, S.; Raghavendra, C.S., "PEGASIS: Power-efficient gathering in sensor information systems," Aerospace Conference Proceedings, 2002. IEEE , vol.3, no., pp.3-1125,3-1130 vol.3, 2002.

[9] Nagarathna, K.; Kiran, Y.B.; Mallapur, J.D.; Hiremath, S., "Trust Based Secured Routing in Wireless Multimedia Sensor Networks," Computational Intelligence, Communication Systems and Networks (CICSyN), 2012 Fourth International

Conference on , vol., no., pp.53,58, 24-26 July 2012.
[10] Christina, D.P.S.E.; Chitra, R.J., "Energy efficient secure routing in wireless sensor networks," Emerging Trends in Electrical and Computer Technology (ICETECT), 2011 International Conference on , vol., no., pp.982,986, 23-24 March 2011.
[11] Ramya, R.; Navamani, T.M.; Yogesh, P., "Secured Identity Based Routing and privacy preservation in Wireless Mesh Networks," Recent Trends in Information Technology (ICRTIT), 2011 International Conference on , vol., no., pp.521,526, 3-5 June 2011.
[12] Jing Dong; Curtmola, R.; Nita-Rotaru, C., "Secure High-Throughput Multicast Routing in Wireless Mesh Networks," Mobile Computing, IEEE Transactions on , vol.10, no.5, pp.653,668, May 2011.

Ishu Gupta received her B.Tech. degree in Electronics & Communication from RIMT-IET, Mandi Gobindgarh, in 2007, the M.Tech. degree in Computer Science & Engg. from Punjabi University , Patiala, in 2009, and pursuing Ph.D. in Computer Science & Engg. from Punjab Technical University, Jalandhar. She is the assistant Professor, with RIMT-MAEC, Mandi Gobindgarh since 2009.Her research interests include Network Simulation & Modelling,Computer Networks.