ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

Energy Efficient, Power Based, Secured Routing Method for Wireless Sensor Network

Swetha.G [1], Anantha Lakshmi E[2], Uma N[3]

Assistant Professor, Dept of ISE, MVJCE, Bangalore, India[1]

Associate Professor, Dept of ISE, MVJCE, Bangalore, India[2]

Assistant Professor, Dept of CSE, NHCE, Bangalore, India[3]

ABSTRACT:A wireless sensor network is a data communication system that consists of from several to thousands of tiny wireless sensor nodes. These battery-powered sensor nodes cooperate with each other to accomplish data transmission. A variety of wireless sensor networks have been developed for different applications in the recent years. In this paper, a data routing protocol that is energy efficient for secure data transmission in wireless sensor networks is proposed. This paper chooses hop counts and battery power as metrics in order to conserve as much energy as possible. We use Shamir's secret sharing and choose the minimum hop path to deliver the data. The battery power of the sensors is chosen to route data randomly to achieve secure data transmission in a wireless sensor network with compromised nodes.

KEYWORDS: Data Collection, energy-efficiency, Multipath, Security, Wireless Sensor Network.

I. INTRODUCTION

A wireless sensor network is a collection of nodes organized into a co-operative network. The nodes in WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. Each sensor node communicates with its neighbour nodes to accomplish data transmission. Therefore sensors usually scatter in a specific area to collect data. Hop by hop, from one sensor to another the data is collected and transferred. In this way, the collected data is transmitted to a base station for further analysis or for remote monitoring and controlling. Therefore, a routing protocol is needed to ensure the message delivery. Even if there are node failures, a robust routing protocol should dynamically adjust the transmission path accordingly. There has been much research in the field of network layer protocols for wireless sensor networks, such as flooding [1,2], directed diffusion [3], sequential assignment routing [4], There is security threat in such kind of networks, as an adversary can physically compromise a subset of sensor nodes in a WSN to eavesdrop information. These compromised nodes act as a black-hole [5]. Therefore, network security is an important issue to WSNs. As well, these sensors work on battery power, which is limited and therefore the routing algorithm should also be efficient enough to conserve battery power and ensure security. To ensure security, the location of adversary has to be known prior, which is not possible. Hence to locate the adversary, we can use algorithms proposed in [6], but each time running a algorithm to locate a black-hole and then sending data is a overhead and it is difficult to obtain such precise information in practical. Therefore to overcome this drawback, we design a routing protocol that is random and also ensuring secured data transfer using minimum battery power.

The data is delivered using Multipath routing that allows the establishment of multiple paths between a single source and destination node. Multipath routing does not ensure full security, as the adversary can compromise the nodes, by obtaining the information about the algorithm used to construct the multipath routes. Also, once constructed, these paths are fixed from a source to a destination. Therefore, the solution to this problem is delivering information randomly through different paths rather than fixed set of routes [7]. Although the adversary can still intercept part of information, we can reduce the probability of interception to an acceptable extent by some mechanism.

In this paper, we propose a efficient approach of secure data collection for WSN. We use Shamir's secret sharing and a minimum hop routing algorithm based on power to achieve secure data collection in a WSN with compromised nodes.

The proposed routing algorithm makes use of the routing functionality of WSN, to improve the quality of data collection.

II. ENERGY EFFICIENT MULTIPATH ROUTING

Wireless Sensor Network (WSN) is intended for monitoring an environment. The main task of a wireless sensor node is to sense and collect data from a certain domain, process them and transmit it to the sink where the application lies. However, ensuring the direct communication between the sink may force nodes to emit their messages with such a high power that their resources could be quickly depleted. Therefore, the collaboration of nodes to ensure that distant nodes communicate with the sink is a requirement. In this way, messages are propagated by intermediate nodes so that a route with multiple links or hops to the sink is established. Multipath routing has been used for different goals in WSN, such as load balance, energy efficiency, etc.

When the sensor constructs its message packet, it makes use of Shamir's algorithm [8], (t, n)-threshold secret sharing algorithm to encode the data. The sensor node that needs to send data packet (source), first breaks the packet into N shares, according to the algorithm and deliver shares through routing path. Routing can be done as proposed in [7]. But the algorithms in [7] does not consider the density of the nodes, if the degree of sensor node of a source node is small, compared to the shares it divided, there may not be enough neighbouring nodes to deliver shares. As the sensor nodes are randomly distributed over a large area, the degree of every sensor node differs.

The algorithms in [7] PRP, NRP or DRP does not ensure the directionality in their propagation. The shares might be propagated back and forth, or may be propagated far away from the base station. Moreover, when the share travels in the opposite direction of the base station, the last sensor that receives the share needs to use some min-hop routing algorithm to deliver the share to base station, that again consumes most of the energy to propagate the share to the base-station, as the path might be long when the share performed random walk away from the base station. Also, it makes the share to live for long time in the network, so that an adversary can easily get hold of information. These algorithms do not consider the battery of the sensor, which is the important factor to be considered. Hence, the algorithm proposed in [7] is modified to randomly generate routing paths for the collection of data.

The proposed algorithm is energy-efficient, and behaves as a random multipath routing algorithm. The algorithm uses the parent list of every node to deliver data from a source to destination. The randomness is accomplished by choosing a neighbour from the parent list (i.e., in turn indicates the hop count) battery power of sensor [9]. The algorithm is as follows.

The algorithm has two phases. First, the construction and maintenance of the routing information about every node. Second, routing of the data.

In this sensor network model, every sensor maintains a routing table that has the information about all the neighbouring sensors, that is its parent, sibling and child node, "hop" – the hop count between the sending node and base station, along with their energy levels. This is done as a part of sensor network initialisation process, where a sink node broadcasts a setup packet that have a "Setup-ID-Hop-Energy" information.

Initially the energy is set to a very high value and forwarded to all the sensors in one hop distance. These sensors update its routing table with this information. The "Setup" indicates that the packet is a setup packet and "ID" is the ID of the sending node, "hop" is the hop count from the sending node to the base station, "Energy" is the battery power of the sensor. After receiving the setup packet, all the receiving nodes with one hop from base station increments their hop count by 1. These nodes then constructs new setup packet, with the sending node id as the new "ID", and changed hop count as the "Hop" and energy level of the sending node as "Energy". This process repeats until all the nodes in the network are notified. In order to avoid collision from receiving a setup more than once, every sensor waits for some fixed time and then update the routing table. Fixed time is chosen as proportional to the hop count value of the received packet. This also ensures that the sensor can never receive a setup packet that has smaller value than this.

Whenever a sensor detects a change in its energy level (battery power), it sends message to all its neighbours with the changed energy level. Thus the neighbouring nodes update this information in its routing table. In this way every sensor maintains information about its neighbours which is used when routing data. Thus we can use power of a sensor (energy) to select a neighbour to send a share, not only it ensures randomness, but we can also avoid forwarding a share to a sensor that has very less battery power, which would otherwise had drained before transferring a share to its neighbour or would not have enough power to send share to a neighbour within its range.

Second, when a sensor senses data, it constructs data packet, and sends this information or message in disguise (encode), by breaking it into N shares according to Shamir's secret sharing algorithm. Then to perform routing of the shares across the network that has compromised nodes, it uses a routing algorithm that is secure besides being random in nature as follows.

Source uses its routing list, choosing a neighbour that is one among the parents. This also ensures directionality in its propagation. In this way, each sensor selects its parent making k number of hops on each path to reach the base station. In this way for each sensor if there are M parents, then there are M number of paths from the source to base station.

Case 1: when the degree of the sending node (source) i.e., the number of paths M of the source node is greater than the number of shares N, (If M > N)
Then, select the path such that the immediate node to relay is one of the parent, and it has the highest power of other parent nodes. Choosing parent node ensures minimum number of hops to reach the base station. Thus the share is forwarded to this neighbour. In this way every neighbour chooses a neighbour in from its parents list, that has highest power and forwards the share to reach the base station. If the parent nodes does not satisfy the criteria, the sibling are selected using the above procedure.

Every time the sensor receives the share, it updates its parent node from which it received the packet with its new energy level. Thus by selecting neighbour based on power, we ensure randomness and by using the parent list to select a neighbour directionality is ensured. The energy is not wasted by sending to neighbours that is not in the direction of the base station. It also ensures that the message is not moved back and forth in the network living for a long time.

Case 2 : If the number of shares N are greater than the number of parents M (If M <= N)
Then, split the message packet into PS shares, and perform unicasting. For each share again choose a neighbour from its parents list first, if all the parents have already chosen, choose the neighbour from the sibling list. Choosing a neighbour here too involves the sensor with highest power and then forward the share. This neighbour in turn performs the same. In this way the share is propagated from source to destination.

III. ANALYSIS OF ENERGY CONSUMPTION

The wireless sensor node, being equipped with limited battery power, Sensor node lifetime plays a major role in designing any algorithm. The main task of the sensor is to detect events, perform quick processing and then transmit data, power consumption can henceforth be divided into three domains. The power required for sensing the event, power for communication and for the data processing. The sensing power varies in application. The complexity of event detection also varies depending upon the noise levels. Higher the noise level, higher is the energy consumed. Other than these, data communication plays a major role in dissipation of power. The data communication is further divided into transmission and receiving.

Let the energy $E_{(Rx)}$ denote the energy consumed for receiving the data and $E_{(Tx),}$ for transferring the data. To transfer data of size x, the data size in bits, over a distance d (obtained using the distance formula applied on the two coordinates(x1,y1),(x2,y2), the locations of sender and receiver respectively).

$E_{(Rx)}$ can be considered as some constant, say c.(i.e., $E_{(Rx)}= xE_{elec}$, where E_{elec} is the electronics energy) and the $E_{(Tx)}$ (x,d) can be obtained as the x E_{elec} + $xE_{efs}d^2$. Hence the total energy dissipated for transmitting a share across a route is given as

$E_{total} = \sum_{i=0}^{k}(E(rx) + E(tx))$ .... Eq 4.1

Where K are the number of nodes that a share passes through to reach destination.

IV. RELATED WORK

There have been a few of on-going efforts about multipath routing for secure data collection presented in literature. For example, the SPREAD algorithm in [10] attempts to find multiple most-secure and node disjoint paths. A modified Dijkstra algorithm is used to iteratively find the top-K most secure node disjoint paths. The H-SPREAD algorithm [11] improves the SPREAD algorithm by simultaneously accounting for both security and reliability

requirements. Shu et al. in [7] present an approach for secure data collection by using (t, n)-threshold secret sharing algorithm and randomized multipath routes. A packet is broken into shares, which are sent to the sink through randomly generated paths.

V. CONCLUSION

We have presented an energy-efficient and secure routing scheme for wireless sensor networks. The time complicity of the proposed protocol is not discussed because it is beyond the scope of this paper. In the proposed data routing scheme, sensor nodes (source) constructs the message packet and it is then split into shares and propagated to a neighbour. Neighbour is chosen in random based on the node with highest energy and less number of hops to reach the base station. Since the battery power of the network is utilized efficiently and evenly among all the sensor nodes, the lifetime of the wireless sensor networks could be extended to its optimum. Also, as the sensors update itself with its power information in the routing table, we get the optimal path. Therefore, the proposed scheme is robust, energy-efficient and scalable.

REFERENCES

[1] J. N. Al-Karaki and A. E. Kamal, “Routing techniques in wireless sensor networks: A survey,” IEEE Wireless Communications, pp. 6-28, Dec. 2004.
[2] I. F. Akyildiz, S. Weilian, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks,” IEEE Communications Magazine, vol. 40, no. 8, pp. 102-114, 2002.
[3] C. Intanagonwiwat, R. Govindan, and D. Estrin, “Directed diffusion: A scalable and robust communication paradigm for sensor networks,” Proceedings of the ACM Mobi-Com, pp. 56-67, 2000.
[4] K. Sohrabi, J. Gao, V. Ailawadhi, and G. Pottie, “Protocols for self-organization of a wireless sensor network,” IEEE Personal Communications, pp. 16-27, 2000. F.
[5] Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci: A survey on sensor networks, IEEE Communications Magazine, Vol. 40(8), pp. 102–114 (2002).
[6] T. Shu, S. Liu, and M. Krunz: “Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes”, Proc. IEEE INFOCOM Conference, pp. 2846-2850 (2009).
[7] A. Shamir: How to Share a Secret, Communication of the ACM, Vol. 22(11), pp. 612-613 (1979).
[8] Shao-Shan Chiang, Chih-Hung Huang, Kuang-Chiung Chang : “A Minimum Hop Routing Protocol for Wireless Sensor Networks.”
[9] W. Lou, W. Liu, and Y. Fang, “Spread: Enhancing Data Confidentiality in Mobile Ad Hoc Networks,” Proc. IEEE INFOCOM, vol. 4, pp. 2404-2413, Mar. 2004.
[10] W. Lou and Y. Kwon, “H-Spread: A Hybrid Multipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks,” IEEE Trans. Vehicular Technology, vol. 55, no. 4, pp. 1320- 1330, July 2006.
[11] P.C. Lee, V. Misra, and D. Rubenstein, “Distributed Algorithms for Secure Multipath Routing,” Proc. IEEE INFOCOM, pp. 1952- 1963, Mar. 2005.