International Journal of Electronics Communication and Computer Engineering
Volume 3, Issue 5, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

Randomized Routing for Wireless Sensor Networks: Optimized Security and Energy Efficiency

Ch. Suneetha
M.Tech,
Chaitanya Engineering College
Visakhapatnam, A.P., India.

B. Poorna Satyanarayana
Professor, Dept of CSE,
Chaitanya Engineering College,
Visakhapatnam, A.P., India

***Abstract* — A Wireless Sensor Network (WSN) is a wireless network consisting of spatially distributed autonomous devices that use sensors to monitor physical or environmental conditions. Sensor nodes are battery-powered and are expected to operate without attendance for a relatively long period of time. So they must be energy efficient. Sensor networks are also highly susceptible to security attacks. There are mainly two types of attacks on WSNs. They are compromised node attack and denial- of- service attack. To counter these attacks, randomized multi- path mechanism is used. The main advantage of this method is that randomly disjoint multi-path routing does not have a fixed candidate route for selection. Therefore, it is able to ensure that adversaries can not know the routes even if they obtain the routing algorithms in advance. However, this method do not consider the network lifetime of WSNs, which may lead to a high probability of sensor nodes outage and cause a cessation of normal operations. So there is a need to maximize security and make this method energy efficient. In this paper we propose a method that makes the randomized multi- path routing energy efficient and also increases the network security.**

***Keywords* — Black hole, Random routes, Security, Wireless Sensor Network.**

I. INTRODUCTION

Wireless sensor network (WSN) is widely considered as one of the most important technologies for the twenty-first century [1]. In the past decades, it has received tremendous attention from both academia and industry all over the world. A WSN typically consists of a large number of low-cost, low-power, and multifunctional wireless sensor nodes, with sensing, wireless communications and computation capabilities [2][3]. These sensor nodes communicate over short distance via a wireless medium and collaborate to accomplish a common task, for example, environment monitoring, military surveillance, and industrial process control [4]. The basic philosophy behind WSNs is that, while the capability of each individual sensor node is limited, the aggregate power of the entire network is sufficient for the required mission.

In many WSN applications, the deployment of sensor nodes is performed in an ad hoc fashion without careful planning and engineering. Once deployed, the sensor nodes must be able to autonomously organize themselves into a wireless communication network. Sensor nodes are battery-powered and are expected to operate without attendance for a relatively long period of time. In most cases it is very difficult and even impossible to change or recharge batteries for the sensor nodes. WSNs are characterized with denser levels of sensor node deployment, higher unreliability of sensor nodes, and sever power, computation, and memory constraints. Thus, the unique characteristics and constraints present many new challenges for the development and application of WSNs. Due to the severe energy constraints of large number of densely deployed sensor nodes, it requires a suite of network protocols to implement various network control and management functions such as synchronization, node localization, and network security. The traditional routing protocols have several shortcomings when applied to WSNs, which are mainly due to the energy-constrained nature of such networks [4]. For example, flooding is a technique in which a given node broadcasts data and control packets that it has received to the rest of the nodes in the network. This process repeats until the destination node is reached. Note that this technique does not take into account the energy constraint imposed by WSNs. As a result, when used for data routing in WSNs, it leads to the problems such as implosion and overlap [5].

Sensor networks are highly susceptible to denial of service attacks due to their inherent characteristics i.e., low computational power, limited memory and communication bandwidth coupled with use of insecure wireless channel. A black hole attack can be easily launched by an adversary node in the sensor network. The malicious node starts advertising very attractive routes to data sink. The neighbor nodes select the malicious node as the next hop for message forwarding considering it a high quality route and propagate this route to other nodes. Almost all traffic is thus attracted to the malicious node that can either drop it, selectively forward it based on some malicious filtering mechanism or change the content of the messages before relaying it.

Of the various possible security threats encountered in a wireless sensor network (WSN), in this paper, we are specifically interested in combating the attack, compromised node (CN). In the CN attack, an adversary physically compromises a subset of nodes to eavesdrop information. This attack generates black hole: area within which the adversary can either passively intercept or actively block information delivery. Due to the unattended nature of WSNs, adversaries can easily produce such black holes [6]. Severe CN attack can disrupt normal data delivery between sensor nodes and the sink, or even partition the topology.

In this paper our focus is on security and energy efficiency. This paper is organized as follows: Section 2 presents the existing method. Section 3 presents the proposed method. And finally section 4 presents the conclusion.

International Journal of Electronics Communication and Computer Engineering
Volume 3, Issue 5, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

II. EXISTING METHOD

In Randomized multi- path routing method[7], multiple paths are computed in a randomized way each time an information packet needs to be sent, such that the set of routes taken by various shares of different packets keep changing over time. As a result, a large number of routes can be potentially generated for each source and destination. To intercept different packets, the adversary has to compromise or jam all possible routes from the source to the destination, which is practically not possible. Because routes are now randomly generated, they may no longer be node-disjoint. However, the algorithm ensures that the randomly generated routes are as dispersive as possible, i.e., the routes are geographically separated as far as possible such that they have high likelihood of not simultaneously passing through a black hole.

A three-phase approach for secure information delivery in a WSN as illustrated in Figure 1:

• Secret sharing of information,
• Randomized propagation of each information share, and
• Normal routing (e.g., min-hop routing) toward the sink.

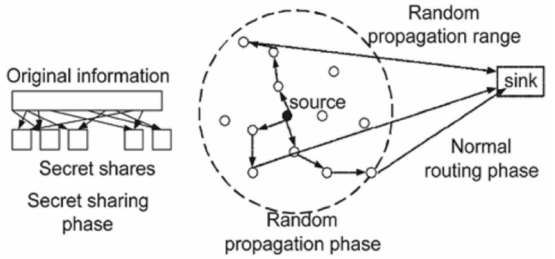

Fig.1. Randomized routing in WSN's

More specifically, when a sensor node wants to send a packet to the sink, it first breaks the packet into M shares, according to a (T, M) -threshold secret sharing algorithm. Each share is then transmitted to some randomly selected neighbor. That neighbor will continue to relay the share it has received to other randomly selected neighbors, and so on. In each share, there is a TTL field, whose initial value is set by the source node to control the total number of random relays. After each relay, the TTL field is reduced by 1. When the TTL value reaches 0, the last node to receive this share begins to route it toward the sink using min-hop routing. Once the sink collects at least T shares, it can reconstruct the original packet. No information can be recovered from less than T shares.

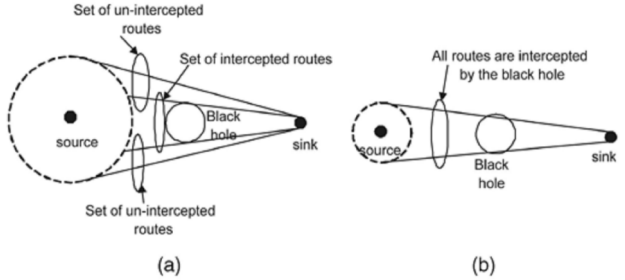

Fig.2. Implication of route depressiveness on bypassing the black hole. (a) Routes of higher depressiveness. (b) Routes of lower dispersiveness.

The effect of route depressiveness on bypassing black holes is illustrated in Figure 2. A larger dotted circle implies that the resulting routes are geographically more dispersive. Comparing the two cases in Figure 2, it is clear that the routes of higher depressiveness are more capable of avoiding the black hole.

The main advantage of this method is that Randomly disjoint multi-path routing does not have a fixed candidate route for selection. Therefore, it is able to ensure that adversaries can not know the routes even if they obtain the routing algorithms in advance. However, this method do not consider the network lifetime of WSNs, which may lead to a high probability of sensor nodes outage and cause a cessation of normal operations. So we need to maximize both the network security and lifetime by exploiting an effective randomly disjoint multi-path routing scheme with secret sharing.

III. PROPOSED METHOD

In this section, we propose a method to maximize both the network lifetime and the security of the randomized multi path routing in WSNs. Specifically, this method focuses on increasing security by utilizing available energy to forward shares with disjoint routes. As the typical many-to-one traffic pattern leads to uneven energy consumption, the sensor nodes close to the sink node have much higher chances of power outage. When one of the sensor nodes is out of energy in WSNs, the nodes far away from the sink node have used only 10% of their batteries. Thus, our proposed scheme aims at utilizing the redundant energy to depressively distribute the shares of packets all over the WSNs, and then forward these shares to the sink node along the randomized disjoint routes. The scheme enhances the network security by increasing the diversity of disjoint routes, which significantly decreases the probability of packet interception by adversaries. In the meantime, the least required number of shares M is reduced with the improvement of security, which leads to energy savings.

The proposed method is composed of three phases:

- Regional dispersive routing
- Disjoint identical hop routing
- Least hop routing

In regional dispersive routing phase, a packet is divided in to M shares. These shares are sent to M randomly selected sensor nodes. In disjoint identical hop routing phase, M shares are transmitted to other sensor nodes dispersively distributed in the network with disjoint routes, where all the sensor nodes along the same routing path have the equal hops to the sink node. Finally, least hop routing phase uses the shortest routing path to forward the M shares to the sink node. As an example all these phases are shown in Figure 3.

International Journal of Electronics Communication and Computer Engineering
Volume 3, Issue 5, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

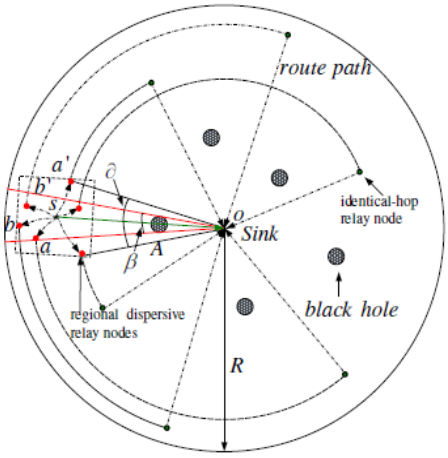

Fig.3. An example of proposed method

Source node s breaks the packet into 6 shares, and sends them to the randomly selected sensor nodes around the source node, namely regional dispersive relay nodes, then these shares are further forwarded to the sensor nodes randomly selected from the whole network, called identical-hop relay nodes, in disjoint identical-hop routing phase. Finally, M shares are transmitted with shortest routing path to the sink node. Our analysis shows the probability that adversary can decode the packet is close to 0 when there exists one black hole in the WSNs. Even when multiple black holes are in the network, the probability that T shares are intercepted by the adversaries is very low as the area of black hole is tiny comparing with the area of whole WSNs. The redundant energy is utilized to forward the shares of packets along disjoint routes in the whole network, which does not have impact on decreasing the network lifetime. Moreover, with the improvement of network security, the network lifetime is extended as the least required number of shares M is reduced.

The following algorithm shows our proposed method:

Algorithm:

Break packets by (T;M)-threshold secret sharing;
for all Data share si do

Xh $\leftarrow$ Random(- $T_{\max}$, $T_{\max}$);

Yh $\leftarrow$ Random(- $T_{\max}$, $T_{\max}$);

r_h $\leftarrow$ Random(- $r_{\max}$, $r_{\max}$);

si $\leftarrow$ {IDi, Xh, Yh, r_h }

while |Xh| > 0 V |Yh| > 0 do
 if |Xh| > 0 then
  Forward si to (Xh, Yh) along X axis by one hop;
  |Xh| = |Xh| - 1;
 end if
 if |Yh| > 0 then
  Forward si to (Xh, Yh) along Y axis by one hop;
  |Yh| = |Yh| - 1;
 end if
end while

while $|r_h|$ > 0 do

Forward si to r_h along the identical-hop route by one hop;

$|r_h| = |r_h| - 1$;

end while
Transmit si to sink node by least-hop routes;
end for

We define the line from the source node to the sink node as X axis and the line orthogonal to X axis at the source node as Y axis. By considering X axis as polar axis, we construct an analogous polar system with the sink node as pole and γ as the hop coordinate, where γ is the hop length from the polar axis along the route consisting of the sensor nodes that have identical hop length to the sink node. Here h denotes the hop length from source to sink. This is shown in Figure 4.

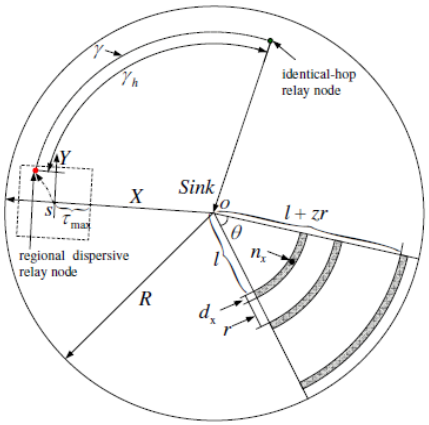

Fig.4. Illustration of regional dispersive and disjoint identical-hop routings.

IV. Conclusion

Advances in Wireless Sensor Network (WSN) technology has provided the availability of small and low-cost sensor nodes with capability of sensing various types of physical and environmental conditions, data processing, and wireless communication. Multi path routing is a technique used for transmitting data in WSNs. However, traditional multi path routing protocols have several shortcomings when applied to WSNs, which are mainly due to the energy-constrained nature of such networks. And also these protocols are vulnerable to various attacks. To counter these attacks, randomized routing is used. Since this method does not consider the network lifetime of WSNS, thus it is not energy efficient. And also some security flaws are there in it. In this paper we provide a method that optimizes the security in randomized routing and also energy efficient.

References

[1] "21 ideas for the 21st century", Business Week, Aug. 30 1999, pp. 78-167.

[2] S.K. Singh, M.P. Singh, and D.K. Singh, "A survey of Energy-Efficient Hierarchical Cluster-based Routing in Wireless Sensor Networks", *International Journal of*

Advanced Networking and Application (IJANA), Sept.–Oct. 2010, vol. 02, issue 02, pp. 570–580.

[3] S.K. Singh, M.P. Singh, and D.K. Singh, "Energy-efficient Homogeneous Clustering Algorithm for Wireless Sensor Network", *International Journal of Wireless & Mobile Networks (IJWMN)*, Aug. 2010, vol. 2, no. 3, pp. 49-61.

[4] Jun Zheng and Abbas Jamalipour, "Wireless Sensor Networks: A Networking Perspective", a book published by A John & Sons, Inc, and IEEEE, 2009.

[5] Luis Javier García Villalba, Ana Lucila Sandoval Orozco, Alicia Triviño Cabrera, and Cláudia Jacy Barenco Abbas, "Routing Protocol in Wireless Sensor Networks", *Sensors* 2009, vol. 9, pp. 8399- 8421.

[6] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks," IEEE Comm. Magazine, vol. 40, no. 8, pp. 102-114, Aug. 2002.

[7] Tao Shu, Student Member, IEEE, Marwan Krunz, Fellow, IEEE, and Sisi Liu, Student Member, IEEE," Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes", IEEE Transactions On Mobile Computing, Vol. 9, No. 7, July 2010.

AUTHOR'S PROFILE

Ch.Suneetha
M.Tech,
Chaitanya Engineering College,
Visakhapatnam, A.P., India

B. Poorna Satyanarayana
Professor, Dept of CSE,
Chaitanya Engineering College,
Visakhapatnam, A.P., India