Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 7, July 2014, pg.823 – 831

RESEARCH ARTICLE

SECURE DATA COLLECTION IN WSN BY RANDOMIZED DISPERSIVE ROUTING

Anil Kumar [1] , Jyoti [2]

1. Assistant Professor, Vaish College of Engineering, Rohtak, Haryana (India)
anilbest2005@gmail.com

2. M.Tech Student, Vaish College of Engineering, Rohtak, Haryana (India)
jyotisoni34@gmail.com

ABSTRACT: ***Various possible security threats that may be experienced by a wireless sensor network (WSN).Compromised-node and denial-of-service are two key attacks in wireless sensor networks (WSNs). In this we study routing mechanisms that circumvent (bypass) black holes formed by these attacks. We argue that existing multi-path routing approaches are vulnerable to such attacks, mainly due to their deterministic nature. So once an adversary acquires the routing algorithm, it can compute the same routes known to the source, and hence endanger all information sent over these routes. In this paper, we develop mechanisms that generate randomized multipath routes. Under our design, the routes taken by the "shares" of different packets change over time. So even if the routing algorithm becomes known to the adversary, the adversary still cannot pinpoint the routes traversed by each packet. Besides randomness, the routes generated by our mechanisms are also highly dispersive and energy efficient, making them quite capable of bypassing black holes at low energy cost. Extensive simulations are conducted to verify the validity.***

KEYWORDS: ***Compromised Node (CN), Denial of service (DOS), Wireless Sensor Networks (WSN), Purely Random Propagation (PRP)***

INTRODUCTION

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions to cooperatively pass their data through the network to a main location. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring, control, and machine health monitoring. The WSN is built of nodes from a few to several hundreds or even thousands, where in each node is connected to one (or sometimes several) sensors.

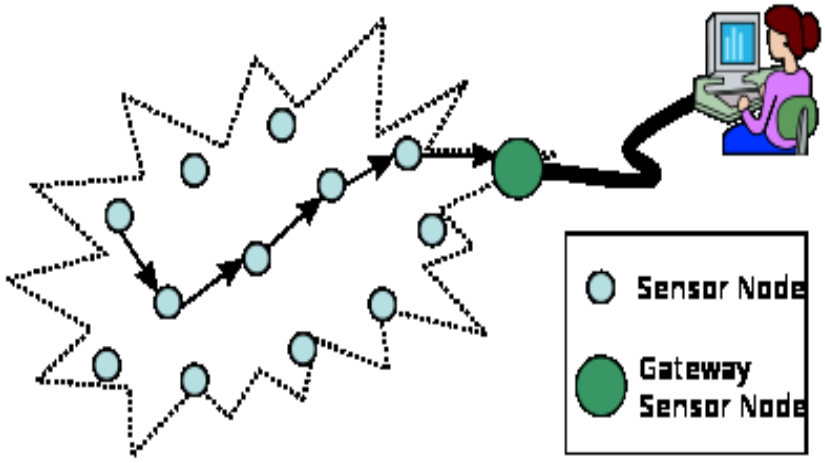

Figure 1: Typical multi-hop wireless sensor network architecture

A denial-of-service attack (**DoS attack**) or distributed denial-of-service attack **(DDoS attack**) is an attempt to make a computer resource unavailable to its intended users. A denial-of-service attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. There are two general forms of DoS attacks: those that crash services and those that flood services. A DoS attack can be perpetrated in a number of ways. The five basic types of attack are:

• Consumption of computational resources, such as bandwidth, disk space, or processor time.

• Disruption of configuration information, such as routing information.

• Disruption of state information, such as unsolicited resetting of TCP sessions.

• Disruption of physical network components.

• Obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

Compromised-node is another attack in wireless sensor network. A node compromise attack often consists of three stages:

i. The first stage is physically obtaining and compromising the sensors.

ii. The second stage is redeploying the compromised nodes back to the sensor network.

iii. The last stage is compromised sensors rejoining the network and launching attacks.

These two attacks are similar in the sense that they both generate black holes and the areas within which the opponent can either passively intercept or actively block information delivery. The objective of our study is to propose a randomized multi-path routing algorithm that can overcome the black holes formed by Compromised-node and denial-of-service attacks. Instead of selecting paths from a pre-computed set of routes, our aim is to compute multiple paths 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 infeasible.

A conventional cryptography-based security method cannot alone provide satisfactory solutions to these problems. This is because once a node is compromised; the adversary can always acquire the secret keys of that node, and thus can intercept any information passed through it. At the same time, an rival can always perform certain form of DOS attack (e.g., jamming) even if it does not have any knowledge of the crypto-system used in the WSN. One solution to these attacks is to exploit the network's routing functionality. Specifically, if the locations of the black holes are known a priori, then data can be delivered over paths that bypass these holes, whenever possible. We argue that three security problems exist in the above counter attack approach:

- First, this approach is no longer valid if the adversary can selectively compromise or jam nodes. This is because the route computation in the above multipath routing algorithms is deterministic for a fixed topology, a fixed set of routes are always computed by the routing algorithm for given source and destination.

- Second, as pointed out in, actually very few node-disjoint routes can be found when node density is moderate and source and destination nodes are several hops apart. The lack of enough routes significantly undermines the security performance of this multipath approach.

- Third, even worse, because the set of routes is computed under certain constraints, the routes may not be spatially dispersive enough to avoid a moderate-sized black hole.

In this paper, we propose a randomized multipath routing algorithm that can overcome the above problems. In this algorithm, multiple paths are created in a randomized way whenever an information packet needs to be sent, such that the set of routes taken by various shares of different packets keep changing time to time and a large number of routes can be potentially generated for each source and end. To intercept different packets, the opponent has to compromise or jam all possible routes from the source to the destination, which is practically impossible.

• 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. Considering the stringent constraint on energy consumption in WSNs, the main challenge in our design is to generate highly dispersive random routes at low energy cost.

Due to Security considerations, we also require that the route computation be implemented in a distributed way, such that the final route represents the aggregate decision of all the nodes participating in the route selection. As a result, a small number of compromised nodes cannot dominate the selection result. In addition, for efficiency purposes, we also require that the randomized route selection algorithm only incurs a small amount of communication overhead.

EXISTING SYSTEM

SPREAD algorithm in attempts to find multiple most-secure and node-disjoint paths. The security of a path is defined as the likelihood of node compromise along that path, and is labeled as the weight in path selection. The H-SPREAD algorithm improves upon SPREAD by simultaneously accounting for both security and reliability requirements. Distributed Bound-Control and Lex-Control algorithms, which computes multiple paths, respectively,

in such a way that the performance degradation is minimized when a single-link attack or a multi-link attack happens, respectively. Flooding is the most common randomized multi-path routing mechanism. To reduce unnecessary retransmissions and improve energy efficiency, the Gossiping algorithm was proposed as a form of controlled flooding, whereby a node retransmits packets according to a pre-assigned probability. Parametric Gossiping was proposed in to overcome the percolation behavior by relating a node's retransmission probability to its hop count from either the destination or the source. When used to counter compromised-node attacks, flooding, Gossiping, and parametric Gossiping actually help the adversary intercept the packet, because multiple copies of a secret share are dispersed to many nodes.

DISADVANTAGES

Existing randomized multi-path routing algorithms in WSNs have not been designed with security considerations in mind, largely due to their low energy efficiency.

Multi-path routing mechanism, Gossiping algorithm has a percolation behavior, in that for a given retransmission probability, either very few nodes receive the packet, or almost all nodes receive it.

The Wanderer algorithm has poor energy performance, because it results in long paths.

PROPOSED SYSTEM

Our proposed solution is to establish a randomized multi-path routing algorithm that can overcome the black holes formed by Compromised-node and denial-of-service attacks.

Instead of selecting paths from a pre-computed set of routes, our aim is to compute multiple paths 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 infeasible.

RANDOM PROPAGATION TECHNIQUES

There are four following distributed schemes for random propagation.

Purely Random Propagation (PRP)

Directed Random Propagation (DRP)

Non-Repetitive Random Propagation (NRRP)

Multicast Tree-assisted Random Propagation (MTRP).

PRP utilizes only one-hop neighborhood information and provides baseline performance.

DRP utilizes two-hop neighborhood information to improve the propagation efficiency, leading to a smaller packet interception probability.

NRRP achieves the same effect, but in a different way: it records all traversed nodes to avoid traversing them again in future.

MTRP tries to propagate shares in the direction of the sink, making the entire delivery process more energy efficient.

PROPOSED ALGORITHM:

For secure information delivery we have three phase approach

- Secret sharing of information
- Randomized propagation of information share
- Normal routing (min hop) towards the sink

STEP1. 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, e.g., the Shamir's algorithm. Each share is then transmitted to some randomly picked neighbor.
STEP2. For random propagation I used the DRP technique for multipath routing. That neighbor will continue to relay the share it has received to other randomly picked neighbors, and so on. In each information share, there is a TTL field, whose initial value is set by the source node to control the total number of randomized relays. After each relay, the TTL field is reduced by 1. When the TTL count reaches 0, the final node receiving this share stops the random propagation phase.
STEP3. When final node receive the share then it route this share towards the sink using normal single-path routing. Once the sink collects at least *T* shares, it can inversely compute the original information. No information can be recovered from less than *T* shares.

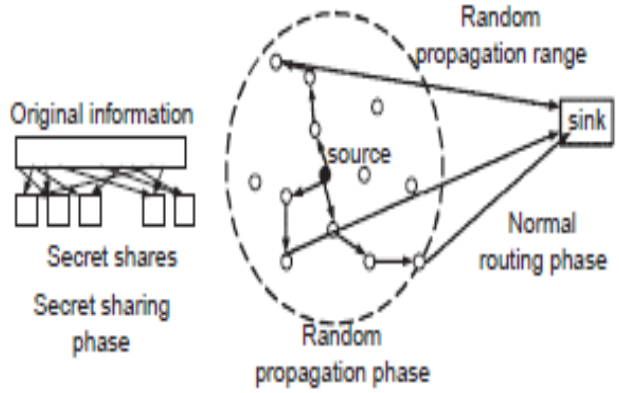

Fig 2.Randomized Dispersive Routing

The effect of route dispersiveness on bypassing black holes is illustrated in Fig.1, where the dotted circles represent the ranges the secret shares can be propagated to in the random propagation phase. A larger dotted circle implies that the resulting routes are geographically more dispersive. It is clear that the routes of higher dispersiveness are more capable of avoiding the black hole.

ADVANTAGES

- Provides highly dispersive random routes at low energy cost without generating extra copies of secrete shares.
- If the routing algorithm becomes known to the adversary, the adversary still cannot pinpoint the routes traversed by each packet
- Energy efficient

Here I used the DRP scheme for propagation of information.
Among the three different routes taken by shares, the route on the bottom right is the most energy efficient because it is the shortest end-to-end path. So, in order to improve energy efficiency, shares should be best propagated in the direction of the sink. And reduce packet interception probability as shown below.

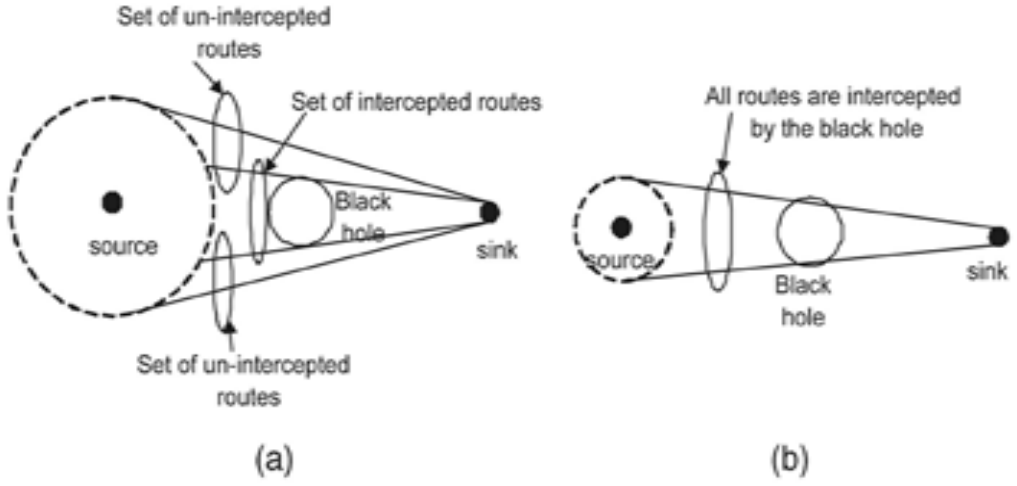

Fig 3. Interception Probability comparison

SIMULATION AND RESULT

The simulation is done with the help of NS-2 (v-2.34) network simulator. The implementation of the protocol has been done using C++ language in the backend and TCL language in the frontend on the fedora Linux operating system. Simulation results are shown in nam window(network animator) using the commands in terminal window.

No. of nodes	**82**
Area size	**1451*1000**
No. of black hole nodes	**1**
Mac	**802.11**
Routing protocol	**DSR**
Simulation time	**5.0 msec**
Traffic source	**CBR**
Transmitting power	**2.0**
Receiving power	**1.5**
Sleep power	**0.5**
Initial energy	**100**

TABLE1: SIMULATION PARAMETERS

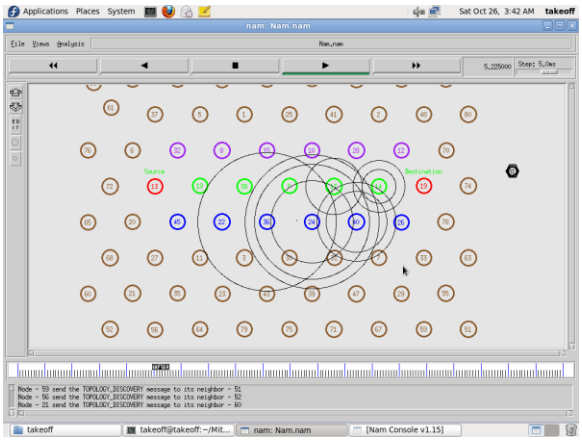

Fig 4.Transmission in multipath routing

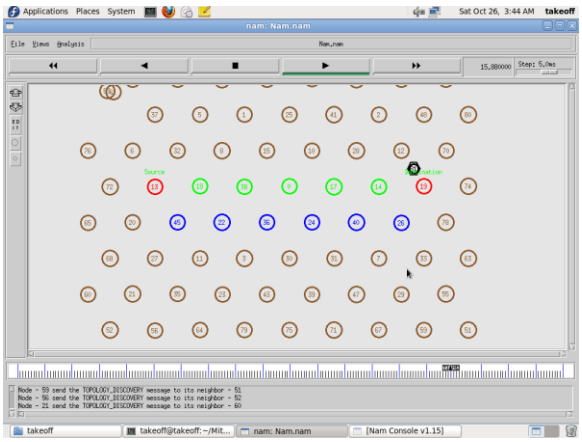

Fig 5.Black hole attack

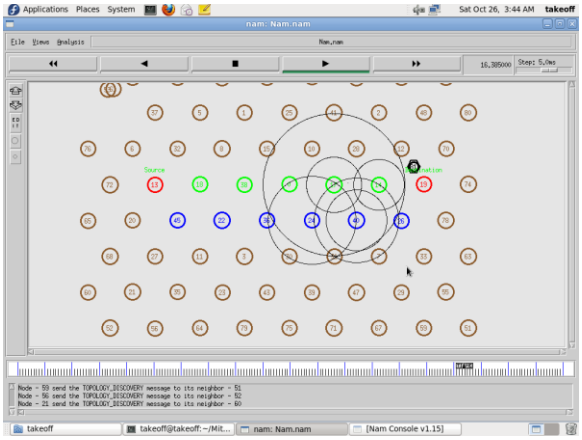

Fig 6.multipath routing after black hole attack

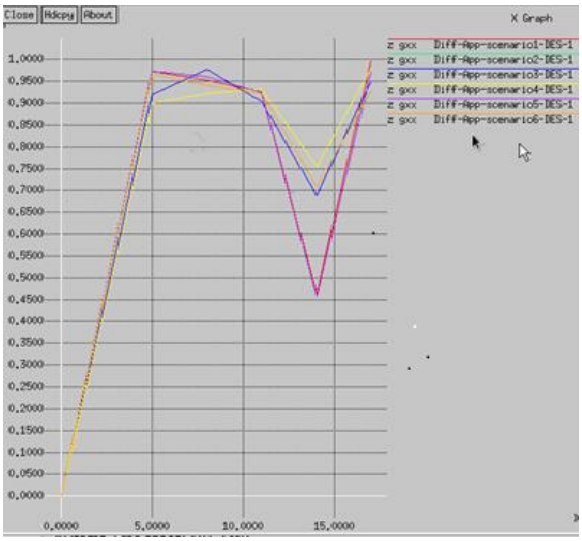

Fig 7. Throughput graph of multipath routing

This throughput xgraph count all the received application packets in a network such that we can calculated the network throughput.

CONCLUSION

By appropriately setting the secret sharing and propagation parameters, I bypass the blackholes generated by both wireless sensor network attacks. By cutting the path which is known to blackhole we can securely transmit the packets because packets on the path known to blackhole change their path. And that changed path is unknown to blackhole.

REFERENCES

[1]I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. IEEE Communications Magazine, 40(8):102–114, Aug. 2002.

[2] C. L. Barrett, S. J. Eidenbenz, L. Kroc, M. Marathe, and J. P. Smith. Parametric probabilistic sensor network routing. In Proceedings of the ACM International Conference on Wireless Sensor Networks and Applications (WSNA), pages 122–131, 2003.

[3] M. Burmester and T. V. Le. Secure multipath communication in mobile ad hoc networks. In Proceedings of the International Conference on Information Technology: Coding and Computing, pages 405–409, 2004.

[4] X. Y. Li, K. Moaveninejad, and O. Frieder. Regional gossip routing wireless ad hoc networks. ACM Journal of Mobile Networks and Applications, 10(1-2):61–77, Feb. 2005.

[5] W. Lou and Y. Kwon. H-spread: a hybrid multipath scheme for secure and reliable data collection in wireless sensor networks. IEEE Transactions on Vehicular Technology, 55(4):1320–1330, July 2006.

[6] W. Lou, W. Liu, and Y. Fang. Spread: enhancing data confidentiality in mobile ad hoc networks. In Proceedings of the IEEE INFOCOM Conference, volume 4, pages 2404–2413, Mar. 2004.

[7] R. Mavropodi, P. Kotzanikolaou, and C. Douligeris. Secmr- a secure multipath routing protocol for ad hoc networks. Elsevier Journal of Ad Hoc Networks, 5(1):87–99, Jan. 2007.

[8] P. Papadimitratos and Z. J. Haas. Secure routing for mobile ad hoc networks. In Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), 2002.

[9] D. R. Stinson. Cryptography, Theory and Practice. CRC Press, 2006.

[10] B. Vaidya, J. Y. Pyun, J. A. Park, and S. J. Han. Secure multipath routing scheme for mobile ad hoc network. In Proceedings of IEEE International Symposium on Dependable, Autonomic and Secure Computing, pages 163–171, 2007.

[11] A. D. Wood and J. A. Stankovic. Denial of service in sensor networks.IEEE Computer Magazine, 35(10):54–62, Oct. 2002.

[12] Z. Ye, V. Krishnamurthy, and S. K. Tripathi. A framework for reliable routing in mobile ad hoc networks. In Proceedings of the IEEE INFOCOM Conference, volume 1, pages 270–280, Mar. 2003.

[13**]** Marc Greis, "Tutorial for the UCB/LBNL/VINT Network Simulator ns."

