IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 2, Apr-May, 2014
ISSN: 2320 – 8791 (Impact Factor: 1.479)
www.ijreat.org

Reliable and Secure Data Gathering in Wireless Sensor Network Using Randomized Spread Routing

Sathiya.M.J[1]

[1]**Department of Electronics and Communication and Engineering, Anna University, CEG Campus**

Abstract

In this paper, we study routing mechanisms that circumvent (bypass) black holes formed by denial of service and compromised node of attacks. The 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. Shamir's algorithm is used in order to have security considerations. 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. In order to provide energy efficiency we use gossiping algorithm which retransmits the packets, thereby improving the energy efficiency.

Index Terms—*Randomized multipath routing, wireless sensor network, secure data delivery.*

INTRODUCTION

Of the various possible security threats that may be experienced by a wireless sensor network (WSN), in this paper we are specifically interested in combating two types of attacks: the compromised-node (CN) attack and the denial-of-service (DOS) attack [3]. The CN attack refers to the situation when an adversary physically compromises a subset of nodes to eavesdrop information, whereas in the DOS attack, the adversary interferes with the normal operation of the WSN by actively disrupting, changing, or even destroying the functionality of a subset of nodes in the system. These two attacks are similar in the sense that they both generate black holes: areas within which the adversary can either passively intercept or actively block information delivery. Due to the unattended method cannot alone provide satisfactory solutions to these problems.

This is because, by definition, once a node is compromised, the adversary can always acquire the encryption/decryption keys of that node, and thus can intercept any information passed through it. At the same time, an adversary 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.

The remedial solution to these types of attacks is to exploit the network's routing functionality. If we know the locations of the black hole formed by compromised (or jammed) nodes are known in priori, then the information can be delivered over the paths that circumvent (bypass) these holes, whenever possible. It is difficult to implement in practice, because of acquiring such location information, the above idea can be implemented in a probabilistic manner, and it consists of a two-step process: secret sharing and multi-path routing. First, information (e.g., a packet) is broken into M shares (i.e., components of a packet that carry partial information) using a (T;M)-threshold secret-sharing mechanism such as the Shamir's algorithm [10]. The original information can be recovered from a combination of at least T shares, but no information can be guessed from less than T shares. Then, multiple routes from the source to the destination are computed according to some multi-path routing algorithm (e.g., [7], [6], [4], [13]). These routes are node-disjoint or maximal node-disjoint subject to certain constraints (e.g., minhop routes). The M shares are then distributed across these routes and delivered to the destination, following different paths. As long as at least M ¡T +1 (or T) shares bypass the compromised (or jammed) nodes, the adversary cannot acquire (or deny the delivery of) the original information packet. 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 in the sense that for a fixed topology, a fixed set of routes are always computed by the routing algorithm for given source and destination. Therefore, even if the shares can be distributed over different routes, overall they are always delivered over the same set of routes that are computable by the algorithm. As a result, once the routing algorithm becomes open to the adversary (this can be done, e.g., through a memory interrogation of the compromised nodes), the adversary can by itself compute the set of routes for any given source and destination. Then the adversary can pinpoint to one particular node in each route and compromise (or jam) these nodes. Such an attack can intercept all shares of the information,rendering the above counter-attack approaches ineffective. Second, as pointed out in [13], actually very few node-disjoint routes can be found when node density is moderate and source and destination nodes are several hops apart. For example, for a node degree of 8, on average only two node-disjoint routes can be found between a source and a destination that are at least 7 hops apart. There is also a 30% possibility that no node-disjoint paths can be found between the source and the destination [13]. The lack of enough routes significantly undermines the security performance of this multipath approach. Last, even worse, because the set of routes is computed under certain constraints, the routes may not be spatially dispersive enough to circumvent a moderate-sized black hole. In this paper, we propose a randomized multi-path routing algorithm that can overcome the above problems. Instead of selecting paths from a pre-computed set of routes, this algorithm computes 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. A large number of routes can be potentially generated for each source and destination. Inorder to intercept different packets, the adversary has to compromise or jam all possible routes from the source to the destination, which is practically infeasible.

The key contributions of this work are as follows. We explore the potential of random dispersion for information delivery in WSNs. Depending on the type of information available to a sensor, we develop four distributed schemes for propagating information "shares": purely random propagation (PRP), directed random propagation (DRP), non-repetitive random propagation (NRRP), and multicast tree-assisted random propagation (MTRP). PRP utilizes only one-hop neighbourhood 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 the future. MTRP tries to propagate shares in the direction of the sink, making the entire delivery process more energy efficient. We conduct extensive simulations to study the performance of the proposed schemes under realistic settings. When their parameters are appropriately set, all four randomized schemes are shown to provide comparable or even better security and energy performance than their deterministic counterparts. At the same time, they do not suffer from pin-pointed node attacks of deterministic multi-path routing.

DATA COLLECTION SYSTEM

The purpose of a data collection system is to allow mobile agents to travel among hosts of a network, to collect

individual data segments from these hosts and to return the set of data segments to the originator of the agent. Each data segment collected by the agent can either be the result of some computation by the agent, based on some local input, or simply the input of some data by the visited host, without any processing by the agent. Our security scheme assures the integrity of data segments against tampering and deletion attacks that might originate from a host visited by the agent, a set of colluding hosts or an intruder on the network. The security of the process used to generate the data segments at each host is out of the scope of our scheme, based on the assumption that, even though each host might behave maliciously against other hosts, each host can be trusted with respect to the generation of its own data. The migration process is another important aspect of the data collection scheme with respect to the security of the collected data. By controlling the migration process, malicious hosts can have a significant impact on the set of data segments collected by the agent. Our data integrity scheme does not address the security of the agent's itinerary. Again, this calls for techniques focusing on the integrity of code execution in untrusted environments as described in [11], [2] and [10] for example.

SECURITY REQUIREMENTS

The data collection process is exposed to a number of attacks from network intruders and legitimate hosts behaving maliciously with respect to competing parties as depicted in [7]. These attacks raise a number of security requirements as follows:

• **Data Integrity**: Di cannot be modified or updated by parties other than Hi.

• **Truncation Resilience**: only the data segments, submitted between the first malicious host Hi and another malicious host Hk can be truncated from the set of data pieces.

• **Insertion Resilience**: no data segment can be inserted unless explicitly allowed.

• **Data Confidentiality**: Di cannot be disclosed to parties other than Hi and H0.

• **Non-Repudiation of Origin**: Hi cannot deny having submitted Di once it was actually included in the set of collected data.

Our definition of the data integrity requirement expands the previous definitions that can be found in [7] and [14] in that a host can update the data it previously submitted. We believe that the update facility is required in free competition and dynamic commercial environments, like stock markets and auctions. The insertion resilience property aims at restricting the number of hosts that can participate thus enabling an elementary access control.

Optimal Secret Sharing and Random Propagation

In this section, we consider the problem of deciding the parameters for secret sharing (M) and random propagation (N) to achieve a desired security performance. To obtain the maximum protection of the information, the threshold parameter should be set as T = M. Then, increasing the number of propagation steps (N) and increasing the number of shares a packet is broken into (M) has a similar effect on reducing the message interception probability. Specifically, to achieve a given Ps (max) for a packet, we could either break the packet into more shares but restrict the random propagation of these shares within a smaller range, or break the packet into fewer shares but randomly propagate these shares into a larger range. Therefore, when the security performance is concerned, a trade off relationship exists between the parameters M and N. On the other hand, although different combinations of M and N may contribute to the same Ps (max) , their energy cost may be different, depending on the parameters Ls, Lp, and q. This motivates us to include their energy consumption into consideration when deciding the secret sharing and random propagation parameters: We can formulate an optimization problem to solve for the most energy-efficient combination of M and N subject to a given security constraint. Formally, this is given as follows:

$$\textbf{minimize } \mathbf{Q^{(PRP)}}$$
$$^{\mathbf{s.t}}\quad \mathbf{P_s{}^{max}\ (M,N) \le P_s{}^{(req)}}$$
$$\mathbf{1\ \square M \square Mmax}$$
$$\mathbf{1\ \square N \square Nmax}$$

where M and N are variables and $Ps^{(req)}$ is the given security requirement. The upper bounds, Mmax and Nmax, are dictated by practical considerations such as the hardware or energy constraints.

EXISTING SYSTEM

The 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. A modified Dijkstra algorithm is used to iteratively find the top- K most secure node-disjoint paths. The H-SPREAD algorithm improves upon SPREAD by simultaneously accounting for both security and reliability requirements.

Flooding is the most common randomized multi-path routing mechanism. As a result, every node in the network receives the packet and retransmits it once. 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 behaviour by relating a node's retransmission probability to its hop count from either the destination or the source. A special form of Gossiping is the Wanderer algorithm, whereby a node retransmits the packet to one randomly picked neighbour. 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 behaviour, 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.

ADVANTAGES:

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

RANDOMIZED MULTIPATH DELIVERY

We consider a three-phase approach for secure information delivery in a WSN as illustrated in fig 1:

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

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 neighbour. That neighbour will continue to relay the share it has received to other randomly selected neighbours, 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.

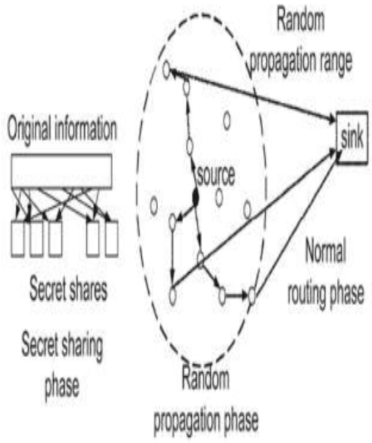
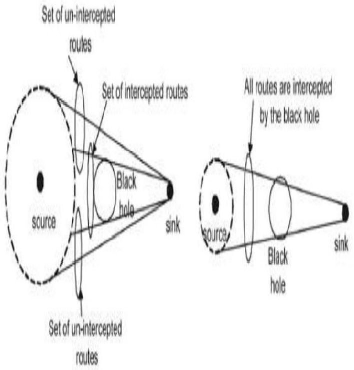


Fig 1: Randomized routing in WSN

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.


Set of un-intercepted routes
Set of intercepted routes
All routes are intercepted by the black hole
Black hole
source
sink
source
Black hole
sink
Set of un-intercepted routes

(a) (b)

Figure 2: Implication of route dispersiveness on bypassing the black hole.
(a)Routes of higher dispersiveness
(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. Clearly, the random propagation phase is the key component that dictates the security and energy performance of the entire mechanism.

CONCLUSION

This paper depicts the effectiveness of the randomized dispersive routing in overcoming the CN and DOS attacks which is energy efficient. By appropriately setting the secret sharing and propagation

References

[1]. 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.
[2]. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. IEEE Communications Magazine, 40(8):102–114, Aug. 2002.
[3]. A. D. Wood and J. A. Stankovic. Denial of service in sensor networks. IEEE Computer Magazine, 35(10):54–62, Oct. 2002.
[4] 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.
[5] 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.
[6] P. C. Lee, V. Misra, and D. Rubenstein. Distributed algorithms for secure multipath routing in attack-resistant networks. IEEE/ACM Transactions on Networking, 15(6):1490–1501, Dec. 2007.
[7] 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.
[8] 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.
[9] 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.
[10] 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.
[11] 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.
[12] D. R. Stinson. Cryptography, Theory and Practice. CRC Press, 2006.
[13] 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.