Secure Data Transmission in Wireless Sensor Network Using Randomized Dispersive Routing Algorithm

Pallavi Motharkar[1], Dr.P.R.Deshmukh[2] and Prof.G.S.Thakare[3]

[1]M.E. (Computer Engineering), [2,3]Department of Computer Science and Engg.
SIPNA COLLAGE OF ENGINEERING AND TECHNOLOGY, AMRAVATI

ABSTRACT

Security threats encountered in a wireless sensor network, so various security providing algorithms are available. In this paper, study of routing mechanisms that circumvent (bypass) black holes formed by these 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. Compromised-node and denial-of-service are two key attacks in wireless sensor networks (WSNs). In this paper, the mechanism is to generate randomized multipath routes. Under this 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 of this mechanism.

Keywords: Denial-of-Service, Randomized Multipath Routes, Sensor network, Circumvent.

1. INTRODUCTION

This is specifically interested in combating two types of attacks: compromised node and denial of service. In the CN attack, 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 network by actively disrupting, changing, or even paralyzing the functionality of a subset of nodes. 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. 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, actually very few node-disjoint routes can be found when the node density is moderate and the source and destination nodes are several hops apart.

Randomized Multipath Routing Methods

1.1 Randomized Multipath Delivery
1.2 Random Propagation of Information Shares

1.1 RANDOMIZED MULTIPATH DELIVERY

This method considers a three-phase approach for secure information delivery in a WSN: 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 threshold secret sharing algorithm. Each share is then transmitted to some randomly selected neighbour [7]. 1. Randomized dispersive routing in a WSN. 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 [4]. The effect of route dispersiveness on bypassing black holes, 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.

1.2 RANDOM PROPAGATION OF INFORMATION SHARES

To diversify routes, an ideal random propagation algorithm would propagate shares as dispersively as possible. Typically, this means propagating the shares farther from their source. At the same time, it is highly desirable to have an energy-efficient propagation, which calls for limiting the number of randomly propagated hops. The challenge here lies in the random and distributed nature of the propagation: a share may be sent one hop farther from its source in a given step, but may be sent back closer to the source in the next step, wasting both steps from a security standpoint. To tackle this issue, some control needs to be imposed on the random propagation process [9].

2. PREVIOUS WORK

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 [5] improves upon SPREAD by simultaneously accounting for both security and reliability requirements. The work in [6], [3] presents distributed Bound-Control and Lex-Control algorithms, which compute the multiple paths in such a way that the maximum performance degradation (e.g., throughput loss) is minimized when a single-link attack or a multilink attack happens, respectively.The work in considers the report fabrication attacks launched by compromised nodes. The work in further considers selective forwarding attacks whereby a compromised node selectively drops packets to jeopardize data availability.

The previous work could be classified into categories. The first category studies the classical problem of finding node-disjoint or edge-disjoint paths. Some examples include the Split Multiple Routing (SMR) protocol [4], multipath DSR [5], and the AOMDV [6] and AODMV algorithms that modify the AODV for multipath functionality. As pointed out in [2], actually very limited number of node-disjoint paths can be found when node density is moderate and the source is far away from the destination [9]. The second category includes recent work that explicitly takes security metrics into account in constructing routes. 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 [1] improves upon SPREAD by simultaneously accounting for both security and reliability requirements.

3. PROPOSED APPROACH AND ARCHITECTURE

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 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.

3.1 Proposed Algorithm

Severe CN and DOS attacks can disrupt normal data delivery between sensor nodes and the sink, or even partition the topology. A conventional cryptography-based security 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. Remedial solution to these attacks is to exploit the network's routing functionality. Location information, the above idea is implemented in a probabilistic manner, typically through a two-step process. First, the packet is broken into M shares (i.e., components of a packet that carry partial information) using a ðT; MÞ-threshold secret sharing mechanism such as the Shamir's algorithm. 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. Second, multiple routes from the source to the destination are computed according to some multipath routing algorithm. These routes are node-disjoint or maximally node-disjoint subject to certain constraints (e.g., min-hop routes). The M shares are then distributed over these routes and delivered to the destination. As long as at least M _ T þ 1 (or T) shares bypass the compromised (or jammed) nodes, the adversary cannot acquire (or deny the delivery of) the original packet.

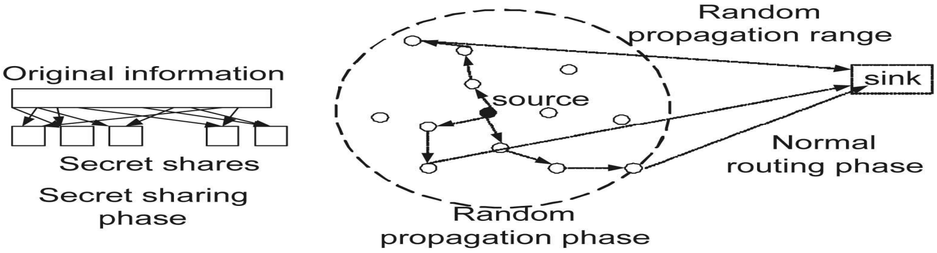

Figure 3.1 Randomized dispersive routing in a WSN.

The effect of route dispersiveness on bypassing black holes is illustrated in Fig., 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.

Randomized Dispersive Routing Algorithm Formula

$$M - T + 1$$

Where,

M= Multiple routes from the source to the destination are computed according randomized routing algorithm.

T = Original information can be recovered from a combination of atleast T shares.

3.2 Advantages of Proposed System

- 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.

3.3Advantages of DDRA Algorithm

- Cost is low compare to cryptographic technique.
- It’s applicable for wired and wireless networks.
- Number of retransmission is less.

4. System Description

Steps for Proposed Approach

1. Enter the number of nodes to form a network.
2. Enter the node name, IP address and port number for each node.
3. Enter the maximum possible paths between the nodes to send the data from source to destination.
4. Login each node to activate it in the network.
5. Enter the source and destination node and select the text file which is to be send.
6. After selecting the files apply the Randomize Dispersive Routing algorithm, which breaks the file into multiple packets and as a result the multiple paths are generated.
7. Each packet is sent through randomized path and all the packets reach to the destination successfully.

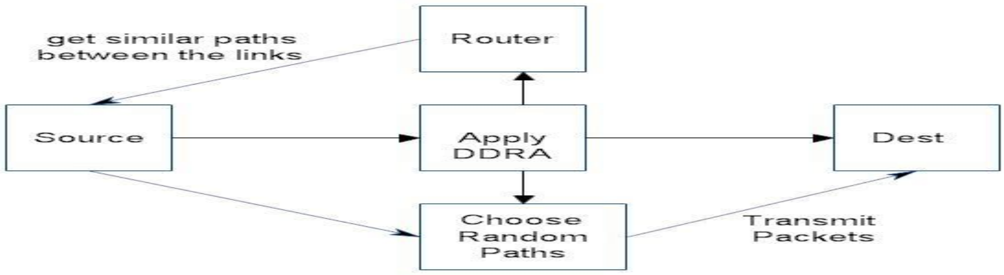

Figure 4.1 System Architecture

Data Flow Diagram:-

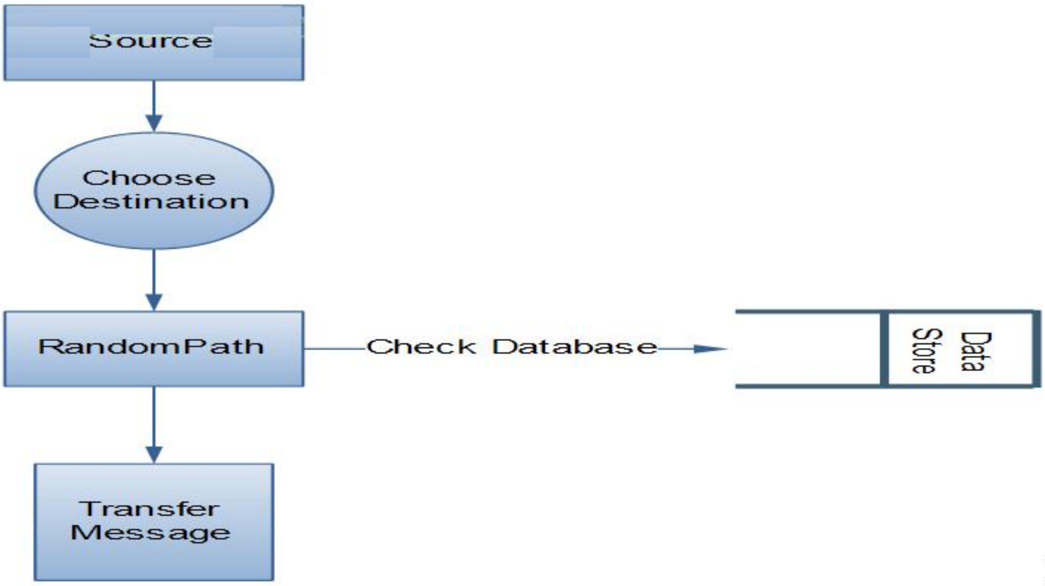

Figure 4.2 Data Flow Diagram

5. Result Analysis

Original file will be split into Multiple Packets and transmitted on multipath by using Randomized Dispersive Rouing Algorithm formula (M – T + 1).It also gives the Acknowledgement to the both sender and receiver that the data is transmitted in fully secure manner and it is Confidential to only that authorized party anyways. According to this Algorithm, description is given in a way that tell us data is fully transmitted and acknowledgment send to sender and receiver.

WHEN 1ST PACKET TRANSFERRED THEN T=5 M=0
M-T+1 = 0-5+1 = - 4 MEANS 4 PACKET YET TO BE RECEIVED
WHEN 2ND PACKET TRANSFERRED THEN T=5 M=1
M-T+1 = 1-5+1 = - 3 MEANS 3 PACKET YET TO BE RECEIVED
WHEN 3RD PACKET TRANSFERRED THEN T=5 M=2
M-T+1 = 2-5+1 = - 2 MEANS 2 PACKET YET TO BE RECEIVED
WHEN 4TH PACKET TRANSFERRED THEN T=5 M=3
M-T+1 = 3-5+1 = - 1 MEANS 1 PACKET YET TO BE RECEIVED
WHEN 5TH PACKET TRANSFERRED THEN T=5 M=4
M-T+1 = 4-5+1 = 0 MEANS ALL PACKET RECEIVED.

The proposed algorithm is easy to implement and compatible with popular routing protocols, such as RIP and others. This proposed algorithm is completely orthogonal to the work based on the designs of cryptography algorithms and system infrastructures. Security enhanced dynamic routing could be used with cryptography-based system designs to further improve the security of data transmission over networks.

6. Conclusion And Future Scope

The effectiveness of the randomized dispersive routing in combating CN and DOS attacks. By appropriately setting the secret sharing and propagation parameters, the packet interception probability can be easily reduced by the proposed algorithms to as low as 10_3, which is at least one order of magnitude smaller than approaches that use deterministic node-disjoint multipath routing. Specifically, the energy consumption of the proposed randomized multipath routing algorithms is only one to two times higher than that of their deterministic counterparts. The proposed algorithms can be applied to selective packets in WSNs to provide additional security levels against adversaries attempting to acquire these packets. Whereby the adversary selectively compromises a large number of sensors that are several hops away from the sink to form clusters of black holes around the sink. Collaborating with each other, these black holes can form a cut around the sink and can block every path between the source and the sink. Our current work does not address this attack. Its resolution requires us to extend our mechanisms to handle multiple collaborating black holes, which will be studied in our future work.

Future Work

- This paper is applicable to transfer only text file data. So in future it can be implemented for other type of files also.

REFERENCE

[1] 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.

[2] C.L. Barrett, S.J. Eidenbenz, L. Kroc, M. Marathe, and J.P. Smith, “Parametric Probabilistic Sensor Network Routing,” Proc. ACM Int’l Conf. Wireless Sensor Networks and Applications (WSNA), pp. 122-131, 2003.

[3] M. Burmester and T.V. Le, “Secure Multipath Communication in Mobile Ad Hoc Networks,” Proc. Int’l Conf. Information Technology: Coding and Computing, pp. 405-409, 2004.

[4] T. Claveirole, M.D. de Amorim, M. Abdalla, and Y. Viniotis, “Securing Wireless Sensor Networks Against Aggregator Compromises,” IEEE Comm. Magazine, vol. 46, no. 4, pp. 134-141, Apr. 2008.

[5] D.B. Johnson, D.A. Maltz, and J. Broch, “DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks,” Ad Hoc Networking, C.E. Perkins, ed., pp. 139-172, Addison-Wesley, 2001.

[6] P.C. Lee, V. Misra, and D. Rubenstein, “Distributed Algorithms for Secure Multipath Routing,” Proc. IEEE INFOCOM, pp. 1952- 1963, Mar. 2005.

[7] P.C. Lee, V. Misra, and D. Rubenstein, “Distributed Algorithms for Secure Multipath Routing in Attack-Resistant Networks,” IEEE/ ACM Trans. Networking, vol. 15, no. 6, pp. 1490-1501, Dec. 2007.

[8] S.J. Lee and M. Gerla, “Split Multipath Routing with Maximally Disjoint Paths in Ad Hoc Networks,” Proc. IEEEInt’1 Conf. Comm. (ICC), pp. 3201-3205, 2001.

[9] X.Y. Li, K. Moaveninejad, and O. Frieder, “Regional Gossip Routing Wireless Ad Hoc Networks,” ACM J.Mobile Networks and Applications, vol. 10, nos. 1-2, pp. 61-77, Feb. 2005.