Wireless Networks Security Using Dispersive Routing Mechanism

[1]Vulupala Sridhar Reddy, [2]M. Venkateswara Rao

[1] Vignana Bharathi Institute of Technology, Department of Information Technology, JNTU-H, Hyderabad, Andhra Pradesh, 501301, India

[2] Vignana Bharathi Institute of Technology, Department of Information Technology, JNTU-H, Hyderabad, Andhra Pradesh, 501301, India

Abstract

Attacks in wireless sensor networks are Compromised-node and denial-of-service (DOS). In the Compromised-node attack (CN attack); an adversary physically compromises a subset of nodes to eavesdrop information, whereas in the denial-of-service 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. Due to the unattended nature of WSNs, adversaries can easily produce such black holes. Severe CN and DOS attacks can disrupt normal data delivery between sensor nodes and the sink, or even partition the topology. In general 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 our Proposal we develop mechanisms that generate randomized multi-path 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.

Keywords: *Compromised-node attack, denial-of-service, Dispersive Routing.*

1. Introduction

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. Due to the unattended nature of WSNs, adversaries can easily produce such black holes. 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.

One remedial 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 circumvent (bypass) these holes, whenever possible. In practice, due to the difficulty of acquiring such 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 (T; M)-threshold secret-sharing mechanism such as the Shamir's algorithm.

Compromised-node and denial-of-service are two key attacks in wireless sensor networks (WSNs). In this paper, 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 of our mechanisms.

2. Overview of Randomized Multipath

We introduce the procedure of Randomized Multi-path delivery mechanism in our paper by including various Modules that support the concept. 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.

The following provides the Architecture of the Routing Mechanism.

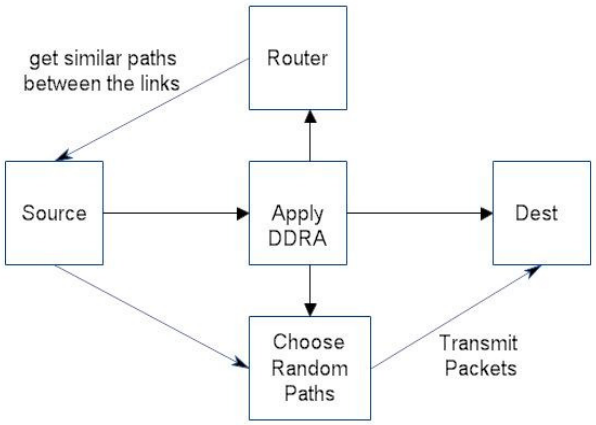

Figure-1: A Simple DDRA procédure

We Propose the following Modules in order to deploy the Routing Mechanism.

2.1 PURE RANDOM PROPAGATION (PRP)

Pure Random Propagation (PRP), shares are propagated based on one-hop neighborhood information. More specifically, a sensor node maintains a neighbor list, which contains the id's of all nodes within its transmission range. When a source node wants to send data to destination, it includes a TTL of initial value N in each share. It then randomly selects a neighbor for each share, and unicasts the share to that neighbor. After receiving the share, the neighbor first decrements the TTL. If the new TTL is greater than 0, the neighbor randomly picks a node from its neighbor list (this node cannot be the source node) and relays the share to it, and so on. When the TTL reaches 0, the final node receiving this share stops the random propagation of this share, and starts routing it toward the sink using normal min-hop routing.

2.2 Non repetitive Random Propagation (NRRP)

- Improves propagation efficiency by recording the nodes traversed so far
- Adds node-in-route (NIR) field to the share header
- Initially NIR is empty at the source node
- When a share is propagated, the ID of the upstream node is added to the NIR field
- Nodes in NIR fields are excluded from random pick at the next hop
- Thus share is relayed to a different node in each step, leading to better Propagation efficiency.

2.3 Directed random propagation (DRP)

- Improves propagation efficiency with two hop neighborhood information
- Adds last-hop-neighbor list (LHNL) field to the header of each share
- Propagating node updates the LHNL field before sending the share
- Receiving node compares this LHNL against its own LHNL & randomly picks
- a node that is not in LHNL of both nodes
- TTL value decremented, LHNL is updated, share relayed
- If the LHNL fully overlaps the relaying node LHNL, a random neighbor is
- Selected, just like PRP.

Benefits

Reduces the chance of propagating a share back and forth
Better propagation efficiency as the share is pushed outwards

2.4 Multicast Tree Assisted Random Propagation (MTRP)

The Traditional location based routing algorithms

- Require location information at both the source and the destination and sometimes intermediate nodes (GPS at each node).
- low accuracy of localization and high cost
- MTRP involves directionality in its propagation without needing location
- information
- Sink constructs a multicast tree from itself to every node
- Each node has a field that records the number of hops to the sink from its neighbor

3. Implementation Procedure

We consider a 3-phase approach for secure information delivery in a WSN: secret sharing of information, randomized propagation of each information share, and normal routing (e.g., minhop 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, e.g., Shamir's 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.

3.1 Secured Delivery of packet

In this module we can maintain the routing table; here we add one more column to maintain the packet delivery ratio. In this one we can maintain how many packets are transmitted over each path. It will be useful for to identify any path can handle number packets. We can stop transmission some amount of time period over that path. So the hacker cannot identify in which path the message is transmitted and also we can easily transmit the data securely.
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. It is well known that the 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.

3.2 Randomized multi-path delivery

We consider a 3-phase approach for secure information delivery in a WSN: secret sharing of information, randomized propagation of each information share, and normal routing (e.g., minhop 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, e.g., Shamir's 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.

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 towards 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. The effect of route depressiveness 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. Comparing the two cases, 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.

3.3 Algorithm Evaluation

In cryptography, a secret sharing scheme is a method for distributing a secret amongst a group of participants, each of which is allocated a share of the secret. The secret can only be reconstructed when the shares are combined together; individual shares are of no use on their own.
More formally, in a secret sharing scheme there is one dealer and n players. The dealer gives a secret to the players, but only when specific conditions are fulfilled. The dealer accomplishes this by giving each player a share in such a way that any group of t (for threshold) or more players can together reconstruct the secret but no group of less than t players can. Such a system is called a (t,n)-threshold scheme. A popular technique to implement threshold schemes uses polynomial interpolation ("Lagrange interpolation"). This method was invented by Adi Shamir in 1979.

Note that Shamir's scheme is provable secure, that means: in a (t,n) scheme one can prove that it makes no difference whether an attacker has t-1 valid shares at his disposal or none at all; as long as he has less than t

shares, there is no better option than guessing to find out the secret.

3.4 Shamir's secret share algorithm

Secret sharing refers to method for distributing a secret amongst a group of participants, each of whom is allocated a share of the secret. The secret can be reconstructed only when a sufficient number of shares are combined together; individual shares are of no use on their own.

More formally, in a secret sharing scheme there is one dealer and n players. The dealer gives a secret to the players, but only when specific conditions are fulfilled. The dealer accomplishes this by giving each player a share in such a way that any group of t (for threshold) or more players can together reconstruct the secret but no group of fewer than t players can. Such a system is called a (t, n)-threshold scheme (sometimes it is written as an (n, t)-threshold scheme).Secret sharing was invented by both Adle Shamir and George Blakely, independent of each other, in 1979.

3.4.1 Secret sharing scheme

A secure secret sharing scheme distributes shares so that anyone with fewer than t shares has no extra information about the secret than someone with 0 shares. Consider the naive secret sharing scheme in which the secret phrase "password" is divided into the shares "pa------," "--ss----," "----wo--," and "------rd,". A person with 0 shares knows only that the password consists of eight letters. He would have to guess the password from 26^8 = 208 billion possible combinations.

A person with one share, however, would have to guess only the six letters, from 26^6 = 308 million combinations, and so on as more persons collude. This system is not a secure secret sharing scheme, because a player with fewer than t shares gains significant information about the content of the secret. In a secure scheme, even a player missing only one share should still face 26^8 = 208 billion combinations.
All secret sharing schemes use random bits. To distribute a one-bit secret among threshold t people, t-1 random bits are necessary. To distribute a secret of arbitrary length entropy of (t-1)*length is necessary.

4. Conclusion

This paper has proposed a security-enhanced dynamic routing algorithm based on distributed routing information widely supported in existing networks. The proposed algorithm is easy to implement and compatible with popular routing protocols, such as RIP and DSDV, over existing infrastructures. We must point out that the proposed algorithm is completely orthogonal to the work based on the designs of cryptography algorithms and system infrastructures. Our simulation results have shown the effectiveness of randomized dispersive routing in combating CN and DOS attacks. By appropriately setting the secret sharing and propagation parameters, the packet interception probability can easily be 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 multi-path routing. At the same time, we have also verified that this improved security performance comes at a reasonable cost of energy. Our security enhanced dynamic routing could be used with cryptography-based system designs to further improve the security of data transmission over networks Appendix Appendixes, if needed, appear before the acknowledgment.

5. Future Scope

We have proposed a security oriented Routing Protocol to which we can enhance by providing the concept of Router Healing Procedures and Methodologies to the dynamic environment .It also concentrates on the control of dynamic events occurring in the society.

References

[1] Tao Shu, Marwan Krunz, and Sisi Liu. Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes. IEEE Mobile Computing, Jul, 2010.

[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] T. Claveirole, M. D. de Amorim, M. Abdalla, and Y. Viniotis. Securing wireless sensor networks against aggregator compromises. IEEE Communications Magazine, pages 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. In C. E. Perkins, editor, Ad Hoc Networking, pages 139–172. Addison- Wesley, 2001.

[6] P. C. Lee, V. Misra, and D. Rubenstein. Distributed algorithms for secure multipath routing. In Proceedings of *the IEEE INFOCOM Conference*, pages 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 Transactions on Networking*, 15(6):1490–1501, Dec. 2007.

Vulupala Sridhar Reddy graduated from SreeNidhi Institute of Science and Technology in 2009 with an M.Tech degree in software engineering from department of computer science and engineering, with seven years of Academic experience, presently working in Vignana Bharathi Institute of Technology as an Assistant Professor in the department of Information Technology. My area of interest includes Network Security and Cloud Computing.

M.Venkateshwar Rao B.Tech IT from VNR Vignana Jyothi Institute of Engineering M.Tech CSE From JNTUH College of engineering Hyderabad with eleven years of Academic experience currently he is Asso.Prof. at Vignana Bharathi Institute Of Technology, guided many UG & PG students. His research areas include Data Mining, Security Issues, Networking, Cloud Computing.