International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 1 Issue 5, July - 2012

Dispersive Routing Mechanism for Securing Data in Wireless Networks

[1] S.Srivalli [2]D.jamuna [3] M.Venkata Krishna Reddy

ABSTRACT: Compromised-node and denial-of-service are two key attacks in wireless sensor networks .In the Compromised-node 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

Wireless Sensor Networks typically consists of a large number of low-cost, low-power, and multifunctional wireless sensor nodes, with sensing, wireless communication capabilities. These sensor nodes communicate the distance via a wireless medium and collaborate to accomplish a common task, for example, environment monitoring, military surveillance, and industrial process control.

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. Wireless sensor network (WSN) is a heterogeneous system combining millions of tiny, inexpensive sensor nodes with several distinguishing characteristics. It is low processing power and radio ranges, permitting very low energy consumption in the sensor nodes, and performing limited and specific sensing and monitoring functions.

However, WSNs form a particular class of ad hoc networks that operate with little infrastructure and have attracted researchers for its development and many potential civilian and military applications such as environmental monitoring, battlefield surveillance, and homeland security. However, designing security protocols is a challenging task for a WSN because of the following unique characteristics: Wireless channels are open to everyone and has a radio interface configured at the same frequency band. Thus, anyone can monitor or participate in the communication in a wireless channel. This provides a convenient way for attackers to break into a network.

A stronger security protocol costs more resources in sensor nodes, which can lead to the performance degradation of applications. In most cases, a trade-off has to be made between security and performance. However, weak security protocols may be easily broken by attackers. A WSN is usually deployed in hostile areas without any fixed infrastructure. It is difficult to perform continuous surveillance after network deployment. Therefore, it may face various potential attacksIn 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 MULTI-PATH DELIVERY

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.

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 :

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., 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, 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., 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, 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 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 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

3.4.Problem Definition

A Compromised node and Denial-of-Service are two key attacks in wireless sensor networks (WSNs). Our model circumvents black holes formed by these attacks. For this, we explore the potential of random dispersion for information delivery in WSNs. Depending on the type of information available to a sensor, we develop our distributed scheme for propagating information "shares" called purely random propagation (PRP). PRP utilizes only one-hop neighborhood information and provides baseline performance. To diversify routes, an ideal random propagation algorithm would propagate shares as depressively as possible. 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 and Initially NIR is empty at the source node

3.5.Objectives :

The objectives of the project are given below

1. The objective of our study 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.
2. 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.
3. 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.

3.6.Limitations of secret sharing schemes

Several secret sharing schemes are said to be information theoretically secure and can be proved to be so, while others give up this unconditional security for improved efficiency while maintaining enough security to be considered as secure as other common cryptographic primitives. For example, they might allow arbitrarily large secrets to be protected by 128-bit shares, since the 2^{128} possible shares are generally considered enough to stymie any conceivable present-day adversary. Common to all unconditionally secure secret sharing schemes, there are limitations:

Each share of the secret must be at least as large as the secret itself. This result is based in information theory, but can be understood intuitively. Given t-1 shares, no information whatsoever can be determined about the secret. Thus, the final share must contain as much information as the secret itself.

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

6.REFERENCES

[1]A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz,"Energy analysis of public-key cryptography for wireless sensor networks," in Third IEEE International Conference on
Pervasive.
[2] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in
mobile ad hoc networks: challenges and solutions," IEEE Wireless Communications, vol. 11, no. 1, pp. 38-47, Feb. 2004.
[3] Adrian Perrig, John Stankovic, and David Wagner. Security in
wireless sensor networks. Commun.ACM, 47(6):53{57, 2004.
[4] D. Carman, B. Matt, D. Balenson, and P. Kruus, "A communications security architecture and cryptographic mechanisms for distributed sensor networks," in DARPA SensIT Workshop. NAI Labs, the Security Research Division
Network Associates, Inc., 1999.
[5] H. Chan, A. Perrig, and D. Song, "Random key predistributionvschemes for sensor networks," in Proceedings of the 2003IEEE Symposium on Security and Privacy. IEEE ComputerSociety, 2003
[6] 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.
[7] 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.
[8] 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.

Author information

S.Srivalli pursuing M.Tech from Jaya Prakash Narayan College of Engineering, .B.Tech from Jaya Prakash Narayan Collge of Engineering. Her areas of Interest are in Wireless Sensor Networks & Networking.

Prof.D.Jamuna, Working as Professor & Head of CSE Dept. Jayaprakash Narayan College of Engineering, Mahabubnagar, M.Tech(SE) from School of Information Technology, JNTUH, Hyderabad. BE(CSE) from Vijayanagara Engineering College, Bellary. Experience 15 Years in Teaching Profession. Her areas of Interest are in Wireless Sensor Networks, Data Mining, Networking and guided M. Tech and B. Tech Students IEEE Projects. She is a Member of CSI. She published 3 papers in International Journals.

M. Venkata Krishna Reddy, Working as Assoc. Professor in CSE Dept. Jayaprakash Narayan College of Engineering, Mahabubnagar, M.Tech(CSE) from Vidya Vikas Institute of Technology, Hyderabad. B.Tech(CSE) from Sri Kottam Tulasi Reddy Memorial College of Engineering, Gadwal. His areas of Interest are in Mobile Adhoc Networks, Data Mining, Networking and guided M. Tech and B. Tech Students IEEE Projects. He published 6 papers in International Journals.