JCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-4, Special Issue-3, May 2016 E-ISSN: 2347-2693

Randomized Routing Algorithms for Secure Data Transmission in Wireless Sensor Networks

[1]Priyanka .B, [2]Mahesh .A

[1,2]*Department of Computer Science & Engineering, SVCE Bangalore, India*

Available online at: www.ijcseonline.org

Abstract— In wireless sensor networks various security threats are encountered, so various security providing algorithms are available. Compromised node and denial of service are the two key attacks in wireless sensor networks. Here, we study routing mechanisms that circumvent 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 know to the source, and hence endanger all information sent over these routes. We develop mechanism 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. Here we propose four algorithms those are purely random propagation, non-repetitive random propagation, direct random propagation and optimized random propagation and we compare the four different algorithm to study the performance. Graphical results are used to verify the effectiveness of our design.

Keywords— Wireless sensor networks, Security, Attacks, Routing.

I. INTRODUCTION

A wireless sensor network consists of mobile hosts equipped with wireless communication devices. The transmission of a mobile host is received by all hosts within its transmission range due to the broadcast nature of wireless communication and Omni-directional antenna. If two wireless hosts are not within the transmission range in ad-hoc networks, other mobile hosts located between them can forward their messages, which effectively build connected networks among the mobile hosts in the deployed area. The use of wireless ad hoc networks also introduces additional security challenges that have to be dealt with. The various possible security threats encountered in a wireless sensor network, we 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. Due to the unattended nature of WSN's 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. Likewise, an adversary can always perform DOS attack even if it does not have any knowledge of the underlying cryptosystem. One remedial solution to these attacks is to exploit the networks routing functionality. Specifically, if the location of the black holes are known a prior, then data can be delivered over paths that circumvent these holes, whenever possible.

Due to the difficulty of acquiring such location information, the above idea is implemented in a probalistic manner, typically through a two-step process. First the packet is broken into M share using 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 that T shares. Second, multiple routes from the source to destination are computed according to some multi-path routing algorithm. These routes are node disjoint or maximally node dis-joint subject to certain constraints. The M shares are then distributed over these routes and delivered to the destination.

As along as a least shares bypass the compromised nodes, the adversary cannot acquire the original 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 multi-path routing algorithms is deterministic in the sense that for a topology and given source and destination nodes, the same set of routes is always computed by the routing algorithm. As a result, once the routing algorithm becomes known to the adversary, the adversary can 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 these nodes. Such an attack can intercept all shares of the information, rending the above counter-attack approaches ineffective. Second, as pointed out in, actually the node density is moderate and the source and destination nodes are several hops apart. The lack of enough routes significantly undermines the security performance of this multipath approach. Last, because the set of routes is computed under certain constraints, the routes may not be spatially dispersive enough to circumvent a moderate size black hole. 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".

Here we propose four algorithms those are Purely Random Propagation (PRP), Directed Random Propagation (DRP), Non-Repetitive Random Propagation (NRRP) and Optimized Random Propagation (ORP) and we compare the four different algorithms to study the performance of the proposed schemes under more realistic setting. Our simulation results are used to verify the effectiveness of our design. When the parameters are appropriately set, all four randomized schemes are shown to provide better security performance at a reasonable energy cost than their deterministic counterparts. At the same time, they do not suffer from the type of attacks faced by deterministic multipath routing.

II. PREVIOUS APPROACHES

In the classic multipath routing approaches are vulnerable to such attacks, mainly due to their deterministic nature. So once the adversary acquires the routing algorithm, it can compute the same routes known to the source, hence making all information sent over these routes vulnerable to its attacks such as compromised node and denial of service [1]. A modified Dijkstra algorithm is used to find iteratively find the top k- most secure node dis-joint paths. The H-SPREAD [3]. Algorithm improves upon SPREAD [2]. Simultaneously by both security and reliability requirements. Bound control and Lex-control algorithms [4]. Computes multiple paths in such a way that maximizes performance degradation throughput loss is minimized when a single link attack and multi-link attack happens, respectively. The previous work can be classified into two categories. The first category studies the classical problem of finding node disjoint or edge disjoint points. Some examples include split multiple routing protocol multiple DSR and the AOVMD algorithms that modify the AOVD for multi path functionality. As pointed out in 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. 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 labled as the weight in path selection. A modified Dijkstra algorithm is used to iteratively find the top-K most secure node disjoint paths.

III. PROPOSED WORK

In our work we 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 precomputed 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 from the source to the 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. The objective of this work is to explore a security enhanced dynamic routing algorithm based on distributed routing information widely supported in existing wired and wireless networks. Security has become one of the major issue for data communication over wired and wireless networks. Different from the past work on the design of cryptography algorithms and system infrastructures, here the proposed dynamic routing algorithms that could randomized delivery paths for data transmission.

The algorithm is easy to implement and compatible with popular routing protocols, such as the routing information protocol wired networks and destination sequenced distance vector protocol in wireless networks, without introducing extra control messages. An analytical study on the proposed algorithm is presented, and a series of simulation experiments are conducted to verify the analytic results and to show the capability of the proposed algorithm. To diversify routes, an ideal random propagation algorithm would propagate shares as depressively 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, wasting both steps from a security standpoint. The following algorithms are developed and compared.

In purely random propagation PRP, shares are propagated based on one-hop neighborhood information. More specifically, a sensor node maintains a neighbor list, which contains the ids of all nodes within its transmission range. When a source node wants to send shares to the sink, it includes a TTL of initial value N in each share. It then randomly selects a neighbor for each share, and unicast 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 and relays the share to it, and so on,. When the TTL reaches 0, the final node receiving this 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.

Non-repetitive routing propagation NRRP is based on PRP, but it improves the propagation efficiency by recording the nodes traversed so far. Specifically, NRRP adds a "node-in-route" field to the header of each share. Initially, this field is empty. Starting from the source node, whenever a node propagates the share to the next hop, the id of the upstream node is appended to the NIR field. Nodes included in NIR are excluded from the random pick at the next hop. This non repetitive propagation guarantees that the share will be relayed to a different node in each step of random propagation, leading to better propagation, leading to better propagation efficiency.

DRP improves the propagation efficiency by using two-hop neighborhood information. More specifically, DRP adds a "last-hop neighbor list" (LHNL), field to the header of each share. Before a share is propagated to the next node, the relaying node first updates the LHNL field ith its neighbor list. When the next node receives the share, it compares the LHNL field against its own neighbor list. When the next node receives the share, it compares the LHNL field against its own neighbor list, and randomly picks one node from its neighbor that are not in the LHNL. It then decrements the TTL value, updates the LHNL field, and relays the share to the next hop, 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 destination using normal min-hop routing.

ORP improves the propagation efficiency by using two-hop neighborhood information. More specifically, it adds a "route trace list" (RTL) field to the header of each share. Before a share is propagated to the next node, the relaying node first updates the RTL field with its neighbor list. When the next node receives the share, it compares the RTL field against its own neighbor list, and randomly picks one node from its neighbor that are not in the RTL. It then decrements the TTL value, updates the RTL field, and relays the share to the next hop, 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 towards the destination using normal min-hop routing.

IV. GRAPHICAL RESULTS

The below figures shows the results of our proposed approach comparing which we say that our proposed algorithm is more efficient than to that of the previous algorithms.

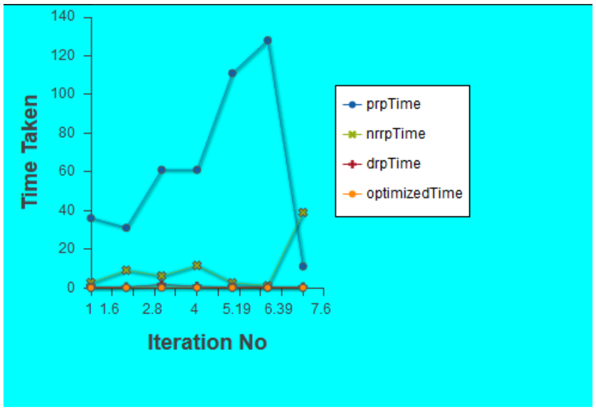

Fig. 1 Time comparison of Algorithms

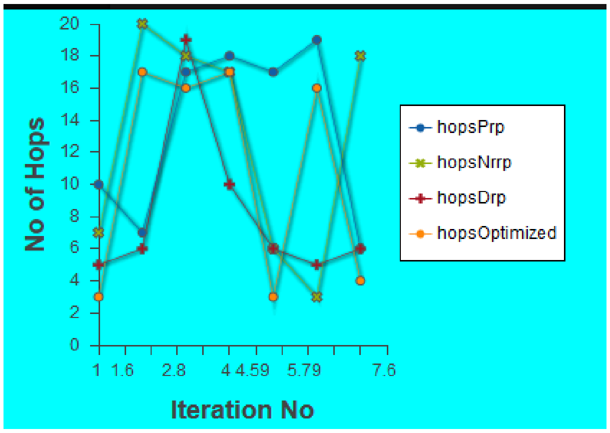

Fig. 2 Hops comparison of Algorithms

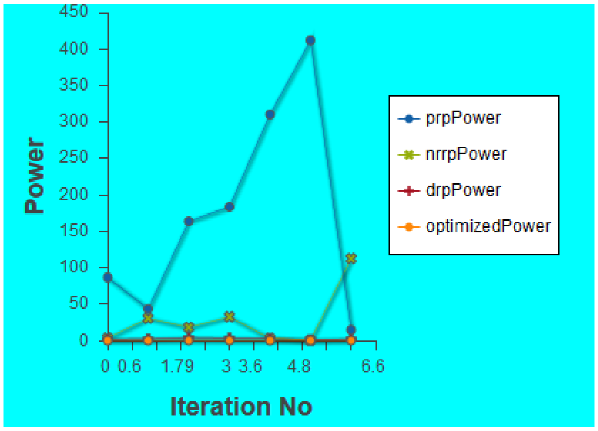

Fig. 3 Power consumption comparison of Algorithms

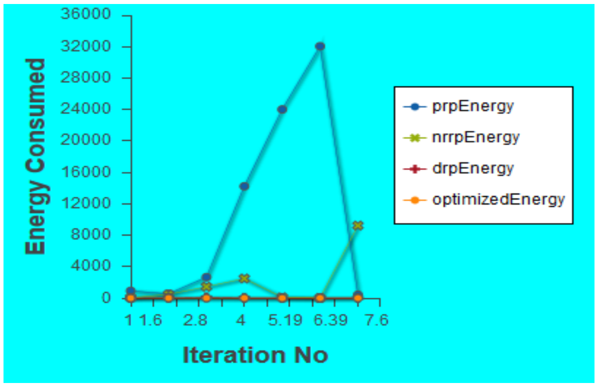

Fig. 4 Energy consumed comparison of Algorithms

FUTURE SCOPE

Our current work is based on the assumption that there are only a small number of black holes in the WSN. In reality, a stronger attack could be formed, whereby the adversary selectively compromises a large number of sensor that are several hops away from the destination to form clusters of black hole around the destination and can block every path between the source and the destination. Under this cut around no secret share from the source can escape from being intercepted by the adversary. Our current work does not address this attack. This resolution requires to extend our mechanisms to handle multiple collaborating black holes.

CONCLUSION

Our analysis and results have shown the effectiveness of the randomized dispersive routing in combating CN and DOS attacks. By appropriately setting the secret sharing and propagation parameters, the number of hops, time energy and power consumed are reduced by the proposed algorithms to and we can find node-disjoint multipath routing. At the same time, we have also verified that this improved security performance comes at a reasonable cost of energy. Specifically, the energy consumption of the proposed randomized multipath routing algorithms is only one to two times higher that of their deterministic counterparts. By adjusting the random propagation and secret sharing parameters different security levels can be provided but our algorithms at different energy costs. Considering that the percentage of packets in a WSN that require a high security level is small, we believe that the selective use of the proposed algorithms does not significantly impact the energy efficiency of the entire system.

REFERENCES

[1] S.G. Santhi and R.Nathiya, "Power Consumption Based Efficient Routing With Mobile Collector in Wireless Sensor Networks", International Journal of Computer Sciences and Engineering, Volume-2(4), Page No (64-70), Apr -2014

[2] W. Lou, W. Liu. Fang, "SPREAD: Enhancing data confidentiality in mobile ad-hoc networks, IEEE INFOCOM 2004, Hong Kong, China, March 2004.

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

[4] P.C. Lee, V. Mishra, and D. Rubenstein. Distributed algorithms for secure multipath routing in attack-resistant networks. IEEE/ACM Transaction on Networking, 15(6):1490-1501, Dec. 2007.

[5] Umesh Kumar Singh, Shivlal Mewada, Lokesh Laddhani and Kamal Bunkar, "An Overview & Study of Security Issues in Mobile Ado Networks", International Journal of Computer Science and Information Security (IJCSIS) USA, Vol-9, No.4, pp (106-111), April 2011

AUTHORS PROFILE

Mahesh A received the M.Tech degree from Visvesvaraya Technological University, Belgaum. Working as an Assistant Professor at Sri Venkateshwara College of Engineering, Area of interest are Wireless Sensor Networks and Cloud Computing.

Priyanka B, PG Scholar at Sri Venkateshwara College of Engineering from the Department of Computer Science of Engineering, Bangalore. Area of interest are Data mining and Wireless Sensor Networks.