Journal of Computer Applications ISSN: 0974 – 1925,
Volume-5, Issue EICA 2012-2, February 10, 2012

Secure Data Delivery in Wireless Sensor Network Using Collaborative Randomized Dispersive Routes

Sabarinathan K
PG Student, Dept ECE,
Mailam Engineering College, Mailam.
Villupuram (Dt).
E-Mail:sabarisysadm@gmail.com

Ramesh S
Assistant Professor, Dept ECE,
Mailam Engineering College, Mailam.
Villupuram (Dt).

Abstract - In wireless sensor networks (WSNs) Compromised-node and denial-of-service are two key attacks that create the black hole in the network. In existing classic multipath routing approaches are vulnerable to such attacks, mainly due to their deterministic nature. 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. In this proposed approach mechanisms that generate randomized multi-path routes, even if the routing algorithm becomes known to the adversary, the adversary cannot pinpoint the routes traversed by each packet. Besides randomness, the generated routes are also highly dispersive and energy efficient, making them quite capable of circumventing black holes. Instead of splitting message into shares, here splitting message into packets and applying MD5 algorithm to provide additional security. The proposed approach provides confidentiality, minimize packet interception probability and end-end energy consumption, the additional features provide solutions to cut-around sink attack.

Keywords: *wireless sensor networks, denial-of-service, routing algorithm.*

I. INTRODUCTION

The various possible security threats encountered in a wireless sensor network (WSN), specifically interested in combating two types of attacks compromised node (CN) and denial of service (DOS).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.

II. EXISTING SYSTEM

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 for a fixed topology, a fixed set of routes are always computed by the routing algorithm for given source and destination.

Second, as pointed out in, actually very few node-disjoint routes can be found when node density is moderate and source and destination nodes are several hops apart. The lack of enough routes significantly undermines the security performance of this multipath approach. Third, even worse, because the set of routes is computed under certain constraints, the routes may not be spatially dispersive enough to avoid a moderate-sized black hole.

III. PROPOSED SYSTEM

These two attacks are similar in the sense that they both generate black holes and the areas within which the opponent can either passively intercept or actively block information delivery. The objective is 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, 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. These two attacks circumvent using randomized multipath routing approach that can minimize packet interception probability and end-end energy consumption. In this approach, data confidentiality provided using key management technique. The additional feature include, it can provide solutions to cut-around sink attack. Randomized multipath routing provided using AODV protocol and key management technique provided using MD5 cryptographic algorithm. The AODV Routing protocol uses an on-demand approach for finding routes, that is, a route is established only when it is required by a source node for transmitting data packets.

The major difference between AODV and Dynamic Source Routing (DSR) stems out from the fact that DSR uses source routing in which a data packet carries the complete path to be traversed. However, in AODV, the source node and the intermediate nodes store the next-hop information corresponding to each flow for data packet transmission. The MD5 Message-Digest Algorithm is a widely used cryptographic hash function that produces a 128-bit (16-byte) hash value. Specified in RFC 1321, MD5 has been employed in a wide variety of security applications, and is also commonly used to check data integrity.

IV. RANDOM PROPAGATION OF INFORMATION SCHEMES

The four distributed schemes for propagating information "packets": 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 neighborhood information and provides baseline performance. DRP utilizes two-hop neighborhood information to improve the propagation efficiency, leading to a smaller packet interception probability. The NRRP scheme achieves a similar effect, but in a different way: it records all traversed nodes to avoid traversing them again in the future. The proposed scheme MTRP tries to propagate packets in the direction of the sink, making the delivery process more energy efficient.

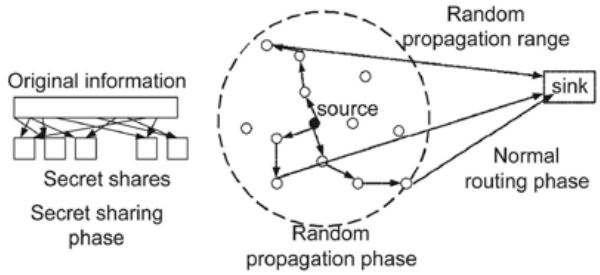

Figure 1: Randomized DispersiveRoutinginaWSN

V. PURELY RANDOM PROPAGATION

In PRP, shares are propagated based on one-hop neighbourhood 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 it 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.

VI. NON REPETITIVE RANDOM 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" (NIR) 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 b relayed to a different node in each step of random propagation, leading to better propagation efficiency.

VII. DIRECTRANDOM PROPAGATION

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 with its 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 neighbors 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. Whenever the LHNL fully overlaps with or contains the relaying node's neighbor list, a random neighbor is selected, just as in the case of the PRP scheme.

VIII. MULTICAST TREE-ASSISTED RANDOM PROPAGATION

MTRP aims at actively improving the energy efficiency of random propagation while preserving the dispersiveness of DRP. Among the three different routes taken by shares, the route on the bottom right is the most energy efficient because it is the shortest end-to-end path. So, in order to improve energy efficiency, shares should be best propagated in the direction of the sink. And reduce packet interception probability as shown below.

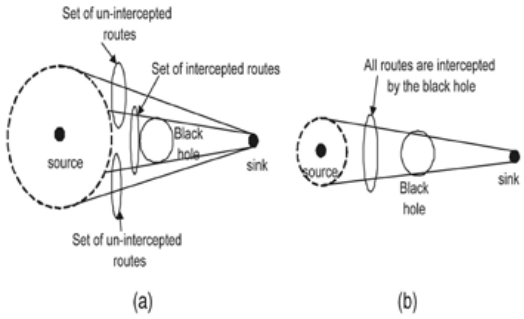

Figure 2: Interception Probability comparison

IX. CONCLUSION

Our analysis and simulation results have shown the effectiveness of the randomized dispersive routing in combating CN and DOS attack. By appropriately setting the key management technique 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. Proposed approach provide confidentiality and minimize packet interception probability.

The implementation of the multicast tree assisted random propagation minimize end-end energy consumption works on collaborative manner and key management technique using MD5 algorithm provide solutions to cut-around sink attack. And the graph study shows the efficiency of MTRP (multicast tree assisted random propagation) scheme.

REFERENCES

1. C.L.Barrett, S.J. Eidenbenz, L.Kroc, M.Marathe, and J.P.Smith, 2003 "Parametric Probabilistic Sensor Network Routing," Proc. ACM Int'l Conf. Wireless Sensor Networks and Applications (WSNA), pp. 122-131.
2. D.B. Johnson, D.A. Maltz, and J. Broch, (2001) "DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks," Ad Hoc Networking, C.E. Perkins, ed., pp. 139-172, Addison-Wesley.
3. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, Aug. 2002 "A Survey on Sensor Networks," IEEE Comm. Magazine, vol. 40, no. 8, pp. 102-114.
4. M. Burmester and T.V. Le, (2004) "Secure Multipath Communication in Mobile Ad Hoc Networks," Proc. Int'l Conf. Information Technology: Coding and Computing, pp. 405-409.
5. P.C. Lee, V. Misra, and D. Rubenstein, Mar. 2005 "Distributed Algorithms for Secure Multipath Routing," Proc. IEEE INFOCOM, pp. 1952-1963.
6. P.C. Lee, V. Misra, and D. Rubenstein, Dec. 2007 "Distributed Algorithms for Secure Multipath Routing in Attack-Resistant Networks," IEEE/ ACM Trans. Networking, vol. 15, no. 6, pp. 1490-1501.
7. S.J. Lee and M. Gerla, 2001 "Split Multipath Routing with Maximally Disjoint Paths in Ad Hoc Networks," Proc. IEEE Int'l Conf. Comm.(ICC), pp. 3201-3205.
8. T. Claveirole, M.D. de Amorim, M. Abdalla, and Y. Viniotis, Apr.2008 "Securing Wireless Sensor Networks Against Aggregator Compromises," IEEE Comm. Magazine, vol. 46, no. 4, pp. 134-141.
9. W. Lou and Y. Kwon, July 2006 "H-Spread: A Hybrid Multipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks", IEEE Trans. Vehicular Technology, vol. 55, no. 4, pp. 1320-1330.
10. X.Y. Li, K. Moaveninejad, and O. Frieder, Feb. 2005 "Regional Gossip Routing Wireless Ad Hoc Networks," ACM J. Mobile Networks and Applications, vol. 10, nos. 1-2, pp. 61-77.