ijecs open access www.ijecs.in
*International Journal Of Engineering And Computer Science ISSN:2319-7242*
*Volume 2 Issue 7 (July 2013), Page No. 2291-2295*

# Multi-Path Routing and Secure Data Collection In Wireless Sensor Networks

***[1]P.Sudhashini, [2]G.Prema, [3]A.Fairosebanu***

Asst.professor Department of Computer science

Rajagiri Dawood Batcha College of Arts and Science Papanasam

Email :vithish88@gmail.com

***Abstract—Multi-path routing establishes multiple paths between a source and destination node in a network. This helps in achieving reliability in mobile ad-hoc networks (MANETs). To achieve efficient, secure and reliable multi-path routing for MANETs, we propose a routing mechanism that uses cross layer strategies. The cross-layer strategy involves incorporating feedback and information from layers below the network layer to make decisions at the network layer. We also propose a path evaluation mechanism for the paths returned by the proposed multi-path routing mechanism. Compromised node and denial of service are two key attacks in wireless sensor networks (WSNs). In this paper, we study data delivery mechanisms that can with high probability circumvent black holes formed by these attacks. We argue that 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. In this paper, we develop mechanisms that generate randomized multipath routes. Under our designs, 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 generated routes are also highly dispersive and energy efficient, making them quite capable of circumventing black holes. We analytically investigate the security and energy performance of the proposed schemes. We also formulate an optimization problem to minimize the end-to-end energy consumption under given security constraints. Extensive simulations are conducted to verify the validity of our mechanisms.***

**Index Terms—**Randomized multipath routing, wireless sensor network, secure data delivery.

## I. INTRODUCTION

### 1.1 Motivations

OF the various possible security threats encountered in a wireless sensor network (WSN), in this paper, we are 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. 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 attacks even if it does not have any knowledge of the underlying cryptosystem. 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 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.

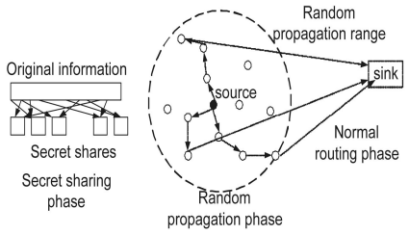
The M shares are then distributed over these routes and delivered to the destination. As long as at least M _ T þ 1 (or T) shares bypass the compromised (or jammed) nodes, the adversary cannot acquire (or deny the delivery of) the original packet. We argue that three security problems exist in the above 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 multipath routing algorithms is deterministic in the sense that for a given 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 (this can be done, e.g., through memory interrogation of the compromised node), the adversary can compute the set of routes for any given source and destination.

Because routes are now randomly generated, they may no longer be node-disjoint. However, the algorithm ensures that the randomly generated routes are as dispersive as possible, i.e., the routes are geographically separated as far as possible such that they have high likelihood of not simultaneously passing through a black hole. Considering the stringent constraint on energy consumption in WSNs, the main challenge in our design is to generate highly dispersive random routes at low energy cost. As explained later, such a challenge is not trivial. A naive algorithm of generating random routes, such as Wanderer scheme (a pure random-walk algorithm), only leads to long paths (containing many hops, and therefore, consuming lots of energy) without achieving good dispersive ness. Due to security considerations, we also require that the route computation be implemented in a distributed way, such that the final route represents the aggregate decision of all the nodes participating in the route selection. As a result, a small number of colluding/compromised nodes cannot dominate the selection result. In addition, for efficiency purposes, we also require that the randomized route selection algorithm only incurs a small amount of communication overhead.

### 1.2 Contributions and Organization

The key contributions of this work are as follows:

1. 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": purely random propagation (PRP), directed random propagation (DRP), no 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. MTRP tries to




propagate shares in the direction of the sink, making the delivery process more energy efficient.

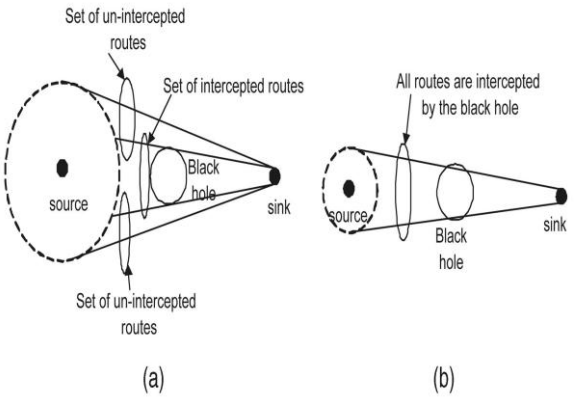
2. We theoretically evaluate the goodness of these dispersive routes in terms of avoiding black holes. We conduct asymptotic analysis (i.e., assuming an infinite number of nodes) for the worst-case packet interception probability and energy efficiency under the baseline PRP scheme. Our results can be interpreted as the performance limit of PRP, and a lower-bound on the performance of the more advanced DRP, NRRP, and MTRP schemes. Our analysis helps us better to understand how security is achieved under dispersive routing. Based on this analysis, we investigate the trade-off between the andom propagation parameter and the secre sharing parameter. We further optimize these parameters to minimize the end-to-end energy consumption under given security constraint.

3. We conduct extensive simulations to study the performance of the proposed schemes under more elastic settings. 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. RANDOMIZED MULTIPATH DELIVERY

### 2.1 Overview

We consider 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 ðT;MÞ-threshold secret sharing algorithm, e.g., Shamir's algorithm. Each share is then transmitted to some randomly selected neighbor. That neighbor will continue to relay the share it has received to 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. The effect of route dispersive ness on bypassing black holes is illustrated in Fig. 2, 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 in Fig. 2, it is clear that the routes of higher dispersive ness 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.

**2.2 Random Propagation of Information Shares**

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, 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.

**2.2.1 Multicast Tree-Assisted Random Propagation**

MTRP aims at actively improving the energy efficiency of random propagation while preserving the dispersive ness of DRP. The basic idea comes from the following observation: 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. In other words, their propagation should be restricted to the right half of the circle in Fig. 1. Conventionally, directional routing requires location information of both the source and the destination nodes, and sometimes of intermediate nodes. Examples of location based routing are the Greedy Perimeter Stateless Routing (GPSR) and Location-Aided Routing (LAR). Location information mainly relies on GPS in each node, or on some distributed localization algorithms. The high cost and the low accuracy of localization are the main drawbacks of these two methods, respectively. MTRP involves directionality in its propagation process without needing location information. More specifically, it requires the sink to construct a multicast tree from itself to every node in the network. Such tree construction is not unusual in existing protocols, and is typically conducted by flooding a "hello" message from the sink to every node. Once the multicast tree is constructed, a node knows its distance (in hops) to the sink and the id of its parent node on the tree. We assume that each entry in the neighbor list maintained by a node has a field that records the number of hops to the sink from the corresponding neighbor. Under MTRP, the header of each share contains two additional fields: maxhop and minhop. The values of these parameters are set by the source to maxhop ¼ ns þ _1 and minhop ¼ ns _ _2, where ns is the hop count from the source to the sink, and _1 and _2 are nonnegative integers with _1 _ _2. The parameter _1 controls the scope of propagation away from the sink, i.e., to the left half of the circle in Fig. 1. The parameter _2 controls the propagation area toward the sink, i.e., the right half of the circle. A small _2 pushes the propagation of a share away from the center line connecting the source and the link and forces them to take the side path, leading to better dispersion.

**III. Asymptotic Analysis of The PRS Scheme**

The random routes generated by the four algorithms in Section 2 are not necessarily node-disjoint. So, a natural question is how good these routes are in avoiding black holes. We answer this question by conducting asymptotic analysis of the PRP scheme. Theoretically, such analysis can be interpreted as an approximation of the performancewhenthe node density is sufficiently large. It also serves as a lower bound on the performance of the NRRP, DRP, and MTRP schemes. Note that the security analyses for the CN and DOS attacks are similar because both of them involve calculating the packet interception probability. For brevity, we only focus on the CN attack model. The same treatment can be applied to the DOS attack with a straightforward modification.

**3.1 Security Definition**

For a given source sensor node, the security provided by the protocol is defined as the worst-case (maximum) probability that for the M shares of an information packet sent from the source, at least T of them are intercepted by the black hole. Mathematically, this is defined as follows: Let the distance between the source s and the sink o be ds. We define a series of N þ 1 circles co centered at s. For the ith circle, 1 _ i _ N, the radius is iRh. For circle 0, its radius is 0. These N þ 1 circles will be referred to as the N-hop neighborhood of s. More specifically we say that a node is i hops away from s if it is located within the intersection between circles i _ 1 and i. We refer to this intersection as ring i. For an arbitrary share, after the random propagation phase, the id of the ring in which the last receiving node, say w, is located is a discrete random variable _ with state space f1; . . .;Ng. The actual path from w to the sink is decided by the specific routing protocol employed by the network. Accordingly, different packet interception rates are obtained under different routing protocols. However, the route given by min-hop routing, which under high node density can be approximated by the line between w and the sink, gives an upper bound on the packet interception rates under all other routing protocols. This can be justified by noting that min-hop routing tends not to distribute traffic over various intermediate nodes and only selects those nodes that are closest to the sink. As illustrated in Fig. 3, this path-concentration effect makes min-hop routing have a smaller traversing area of the paths, and thus is more prone to packet interception, especially when compared to power-balancing routing protocols that build dispersive routes.

**IV. SIMULATION STUDIES**

**4.1 Simulation Setup**

In this section, weuse simulation to evaluate the performance of PRP, NRRP, DRP, and MTRP under more realistic settings. To better understand the capability of these randomized multipath routing algorithms in bypassing black holes, we also compare their performance against a deterministic counterpart, H-SPREAD, which generates node-disjoint multipath routes to combat CN attack in WSNs. We consider a 200 m _ 200 m field that is uniformly covered by sensors. The center of this square is the origin point. All coordinates are in the unit of meters. The sink and the center of the black hole are placed at (100, 0) and (50, 0), respectively. The transmission range of each sensor is Rh ¼ 10 m. For MTRP, we set the parameters _1 ¼ 0 and _2 ¼ 5. In all simulations, after the random propagation phase, each secret share is delivered to the sink using min-hop routing. Each simulation result is averaged over 50 randomly generated topologies. For each topology, 1,000 information packets are sent from the source node to the sink. Our simulation results indicate that the nodes' locations have a significant impact on the absolute value of the packet interception probability of a given scheme. As a result, we emphasize that when reading the simulation results presented below, the absolute value of the mean performance is not as useful as the relative performance ranking between various schemes, and also not as useful as the general trend in performance. Because all comparisons made in our simulations are based on 50 common topologies, this common ground for comparison ensures that our

results preserve the actual relative performance between various schemes.

### 4.2 Simulation Results

#### 4.2.1 Single-Source Case

We first fix the location of the source node at ð_50; 0Þ. In we plot the packet interception probability as a function of the TTL value (N) and the number of shares (M) that each packet is broken into, respectively. The packet interception probability calculated according to our asymptotic analytical model for PRP is also plotted in the same figure for comparison. These figures show that increasing N and M helps reduce the packet interception probability for all proposed schemes. However, for a sufficiently large N, e.g., N ¼ 20 in Fig. 14, the interception probability will not change much with a further increase in N. This is because the random propagation process has reached steady state. It can also be observed that, in all cases, the packet interception probabilities under the DRP, NRRP, and MTRP schemes are much smaller than that of the baseline PRP scheme, because their random propagations are more efficient. In addition, when N and M are large, all four randomized algorithms achieve smaller packet interception probabilities than the deterministic H-SPREAD scheme. In many cases, the gap is more than one order of magnitude. The poor performance of H-SPREAD is due to the small number of node-disjoint routes that can be found by the algorithm when the source is far away from the sink (15 hops apart in our simulation), and the fact that these routes may not be dispersive enough. Increasing M does not change the number of routes the algorithm can find, so it does not help in reducing the interception probability for H-SPREAD. Furthermore, it can be observed that the simulated performance for PRP is reasonably close to its theoretical performance, especially in the medium packet interception- probability regime. This clearly demonstrates that the sample topologies used in our simulations are representative and sufficient, and the

## V. RELATED WORK

The concept of multipath routing dates back to 1970s, when it was initially proposed to spread the traffic for the purpose of load balancing and throughput enhancement. Later on, one of its subclasses, path-disjoint multipath routing, has attracted a lot of attention in wireless networks due to its robustness in combating security issues. The related work can be classified into three 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, multipath DSR, and the AOMDV and AODMV algorithms that modify the AODV for multipath 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. Furthermore, the security issue is not accounted for explicitly in this category of work. The second category includes recent work that explicitly takes security metrics into account in constructing routes. Specifically, the SPREAD algorithm in attempts to find multiple most-secure and node-disjoint paths. 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 improves upon SPREAD by simultaneously accounting for both security and reliability requirements. The work in 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. Both works are based on a similar cryptographic method: the secret keys used by sensor nodes are specific to their geographic locations, which limits the impact of a compromised node. Instead of relying on a cryptographic method for resolving the issue, our work mainly exploits the routing functionality of the network to reduce the chance that a packet can be acquired by the adversary in the first place. Other secure multipath routing algorithms include SRP, SecMR, Burmester's approach, and AODV-MAP. Among them, SRP uses end-to-end symmetric cryptography to protect the integrity of the route discovery; Sec MR protects against the denial-of-service attack from a bounded number of collaborating Malicious nodes; Burmester's method is based on the digital signatures of the intermediate nodes; AODVMAP is another modification of AODV, which can provide local bypass of the attacked nodes.

## VI. CONCLUSIONS

Our analysis and simulation 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 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. 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 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. By adjusting the random propagation and secret sharing parameters (N and M), different security levels can be provided by 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. Our current work is based on the assumption that there is 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 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. Under this cutaround- sink attack, no secret share from the source can escape from being intercepted by the adversary. 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.

## VII. ACKNOWLEDGMENTS

A preliminary version of this paper was presented at the IEEE INFOCOM 2009 Mini-Conference. Part of this work was conducted while M. Krunz was a visiting researcher at the University of Carlos III, Madrid, and IMDEA Networks, Spain. This research was supported in part by the US National Science Foundation (under Grants CNS-0721935, CNS-0904681, and IIP-0832238), Raytheon, and the Connection One" center. Any opinions, findings, conclusions, or recommendations expressed in this paper are those of the author(s) and do not necessarily reflect the views of the US National Science Foundation.

## VIII.REFERENCES

[1] I.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 pplications (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. IEEE Int'l 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.

[10] W. Lou and Y. Kwon, "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, July 2006.

[11] W. Lou, W. Liu, and Y. Fang, "Spread: Enhancing Data Confidentiality in Mobile Ad Hoc Networks," Proc. IEEE INFOCOM, vol. 4, pp. 2404-2413, Mar. 2004.

[12] W. Lou, W. Liu, and Y. Zhang, "Performance Optimization Using Multipath Routing in Mobile Ad Hoc and Wireless Sensor Networks," Proc. Combinatorial Optimization in Comm. Networks, pp. 117-146, 2006.

[13] M.K. Marina and S.R. Das, "On-Demand Multipath Distance Vector Routing in Ad Hoc Networks," Proc. IEEE Int'l Conf. Network Protocols (ICNP), pp. 14-23, Nov. 2001.

[14] R. Mavropodi, P. Kotzanikolaou, and C. Douligeris, "SecMR—a Secure Multipath Routing Protocol for Ad Hoc Networks," Ad Hoc Networks, vol. 5, no. 1, pp. 87-99, Jan. 2007.

[15] N.F. Maxemchuk, "Dispersity Routing," Proc. IEEE Int'l Conf. Comm. (ICC), pp. 41.10-41.13, 1975.

[16] P. Papadimitratos and Z.J. Haas, "Secure Routing for Mobile Ad Hoc Networks," Proc. SCS Comm. Networks and Distributed Systems Modeling and Simulation Conf. (CNDS), 2002.

[17] P. Papadimitratos and Z.J. Haas, "Secure Data Communication in Mobile Ad Hoc Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 343-356, Feb. 2006.

[18] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and D. Tygar, "SPINS: Security Protocols for Sensor Networks," Proc. ACM MobiCom, 2001.