Available online at www.elixirpublishers.com (Elixir International Journal)

Information Technology

Elixir Inform. Tech. 74 (2014) 26780-26786

ISSN: 2229-712X

Data Salvation in Wireless Sensor Networks Using Mesh Topology

Sai krishna Manohar[1,*], M. Srikanth yadav[2], P.Triveni[3], P. Hemalatha[3] and D. Kusuma Naga Anusha[3]

[1]Member of IEEE, ACM, CSI, Department of Information Technology Tirumala Engineering College, Narasaraopet, India.

[2]Life Member of ISTE, Department of Information Technology, Tirumala Engineering College, Narasaraopet, India.

[3]Department of Information Technology, Tirumala Engineering College, Narasaraopet, India.

ARTICLE INFO

Article history:

Received: 16 April 2014;

Received in revised form:

21 August 2014;

Accepted: 29 August 2014;

Keywords

Data salvation,
Message transmission,
Randomized multipath routing,
Mesh topology,
Wireless sensor networks,
Secure data delivery.

ABSTRACT

Security has become one of the major issues for data communication over Wired and Wireless sensor networks. Consider wireless sensor networks while transferring the data it can be attacked by different kinds of attacks such as compromised node, denial of service attacks. We agree that existing multi-path routing approaches are vulnerable to such attacks, mainly due to their deterministic nature. By considering the routing algorithm, it can compute the same routes known to the source, therefore all information sent over these routes. To secure the data from these attacks we can generate randomized multipath routes. These routes are taken by the shares of different packets change over time. While sending the data the randomized multi path routes include the same routes. In this paper, instead of selecting self-nodes we generate dynamic multi path routing in which the shares of different packets are taken and send to the destination. We develop efficient topology for delivery the data in secure manner. The experimental results show that topology out performs traditional schemes in terms of CPU cost, minimization of retransmissions.

Introduction

In wireless sensor network (WAN) while transferring the data it can be attacked by different kinds of attacks. In this paper we are specifically interested to avoid two types of attacks: Compromised node (CN) and denial of service (DOS). In Compromised node attack, an adversary physically compromises a subset of nodes to eavesdrop information, whereas in the Denial of Service attack, the 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 [1]. 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 (e.g., jamming) 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. 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 [20]. 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 [5],[8],[13],[14]. These routes are node-disjoint or maximally node-disjoint subject to certain constraints (e.g., min-hop routes). The M shares are then distributed over these routes and delivered to the destination. As long as at least (M - T + 1) or T shares bypass the compromised (or jammed) nodes, the adversary cannot acquire (or deny the delivery of) the original packet.

Proposed System

In this paper, we propose a randomized multipath routing algorithm that can overcome the above problems. In this algorithm, multiple paths are computed 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 can be potentially generated for each source and destination. To intercept different packets, the adversary has to compromise all possible routes from the source to the destination, which is practically not possible. 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.

The main challenge in our design is to generate highly dispersive random routes at low energy cost. A naive algorithm of generating random routes, such as Wanderer scheme [2] (a pure random-walk algorithm), only leads to long paths (containing many hops, and therefore, consuming lots of energy) without achieving good depressiveness. Due to security considerations, we also require that the route computation 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 compromised nodes cannot dominate the selection result. In addition, for

Tele:
E-mail addresses: saikrisihnamanohar@gmail.com

efficiency purposes, we also require that the randomized route selection algorithm only incurs a small amount of communication overhead. , 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.

Requirement Analysis

We explore the potential of random dispersion for information delivery in WSN. 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), 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. MTRP tries to propagate shares in the direction of the sink, making the delivery process more energy efficient.

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 low-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 random propagation parameter and the secret sharing parameter. We further optimize these parameters to minimize the end-to-end energy consumption under a given security constraint.

We conduct extensive simulations to study the performance of the proposed schemes under more realistic 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.

Randomized Multipath Delivery

Overview

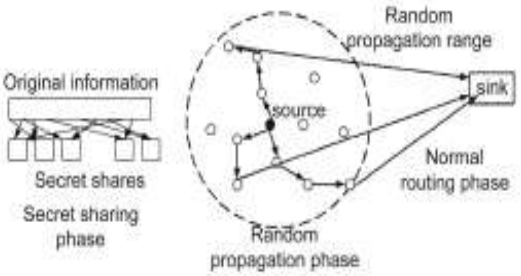

Fig 1. Randomized dispersive routing in a WSN.

As illustrated in the above fig. 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 (T; M) threshold secret sharing Algorithm [20]. 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.

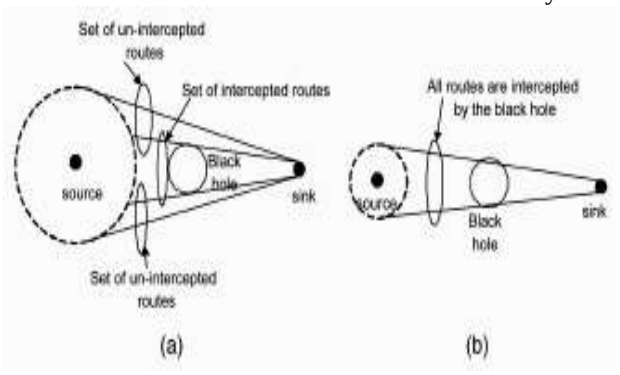

Fig 2: Implication of route depressiveness on bypassing the black hole.

(a) Routes of higher depressiveness.
(b) Routes of lower depressiveness.

` The effect of route depressiveness 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 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.

Random Propagation of data Sharing

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 share may be sent one hop farther from its source in 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.

Purely Random Propagation

In 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 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. The WANDERER scheme [2] is a special case of PRP with $N = \infty$.

Non-repetitive Random Propagation

In NRRP, it is completely 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 be relayed to a different node in each step of random propagation, leading to better propagation efficiency.

Directed Random Propagation

In DRP, it 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. According to this propagation method, DRP reduces the chance of propagating a share back and forth by eliminating this type of propagation within any two consecutive steps.

Multicast Tree-Assisted Random Propagation

In MTRP, we aims at actively improving the energy efficiency of random propagation while preserving the depressiveness of DRP. The basic idea comes from the following observation of Fig. 1: 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.

Asymptotic Analysis Of The Prp Scheme

The random routes generated by the four algorithms in NRRP 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 performance when the 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 analysis for the CN and DOS attacks is 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.

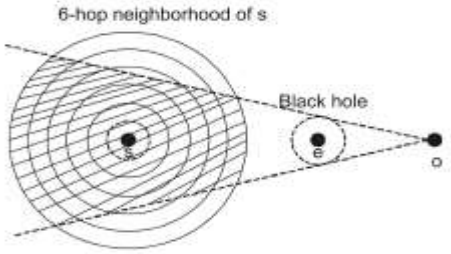

Fig 3: Packet interception area, a six-hop random propagation example.

Models of Network and their Attacks

We consider an area S that is uniformly covered by sensors with density. We assume a unit-disk model for the sensor communication, i.e., the transmitted signal from a sensor can be successfully received by any sensor that is at most Rh meters away. Multi-hop relay is used if the intended destination is more than Rh away from the source. We assume that link-level security has been established through a conventional cryptography-based bootstrapping algorithm, i.e., consecutive links along an end-to-end path are encrypted by symmetric link keys. So, when a node A wants to send a share to its neighbor B, it first encrypts the plaintext using link key KAB and then sends the cipher text to B. When B wants to forward the received share to its neighbor C, it decrypts the cipher text using key KAB, re-encrypts the plaintext using key KBC, then sends it to C, and so on. In this way, the openness of the wireless media is eliminated: a node cannot decrypt a cipher text overheard over the wireless channel if it is not the intended receiver.

We also assume that a link key is safe unless the adversary physically compromises either side of the link. The adversary has the ability to compromise multiple nodes. However, we assume that the adversary cannot compromise the sink and its immediate surrounding nodes. This assumption is reasonable because the sink's neighborhood is usually a small area, and can be easily physically secured by the network operator, e.g., by deploying guards or installing video surveillance/monitoring equipment. Such an assumption is also widely adopted in the literature, e.g., see [18], [23]. We assume that the black hole formed by the compromised nodes can be approximated by its circumcircle, i.e., the smallest circle that encompasses the shape of the black hole. Note that the schemes' operation does not depend on the shape of the black hole. The analysis of the security performance is conservative (i.e., the system is more secure than what it shows by analysis) under this assumption. We denote the circle, its center, and its radius by E, e, and Re, respectively. During the WSN's operation, any end-to-end path that traverses through this circle is considered vulnerable to eavesdropping, i.e., information shares delivered over this path are all acquired by the adversary. In addition, we also assume that the area S is sufficiently large such that the boundary effect of S can be ignored in our analysis. We will consider the boundary effect in our simulations.

Security in data collection using Wireless Sensor Networks

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. As shown in Fig. 3, we define a series of N þ 1 circles concentered at s. For the i^{th} circle, 1 - i - N, the radius is i^{Rh}. For circle 0, its radius is 0. These N + 1 circles will be referred to as the N-hop neighborhood 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. 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.

The worst-case scenario for packet interception happens when the points s, e, and o, in Fig. 3, are collinear (the shaded region denotes the locations of w for which the transmission from w to 0 using min-hop routing will be intercepted by E). Denote the distance between e and o by de. Given ds and de, when s, e, and o are collinear, the shaded region attains its maximum area, and thus gives the maximum packet interception probability. For ring i, denote the area of its shaded portion by Si.

Energy Efficiency of the Random Propagation

We assume that the energy consumption for delivering one bit over one hop is a constant q. Then, the average energy consumption for delivering one packet from source s to sink o depends on the average length (in hops) of the route. Note that each random route consists of two components. The first is a fixed N-hop component attributed to the random asymptotic assumption, when min-hop routing is used, the ratio between the number of hops from w -> o and from s -> o can be approximated by the ratio of the lengths of these two paths.

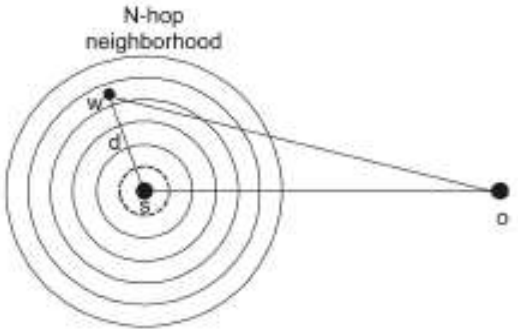

Fig 4: The complete transmission distance after random propagation.

This ratio can be calculated as follows. Suppose w is located in the i^{th} ring (see Fig. 10). Let the distance between w and s be (i-1) Rh<=d<=i^{Rh} simulation studies

Simulation Setup

In this section, we use 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 [10], 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 = 10m. 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.

Simulation Results

Single-Source Case We first fix the location of the source node at (-50,0). In Figs. 14 and 15, 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=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.

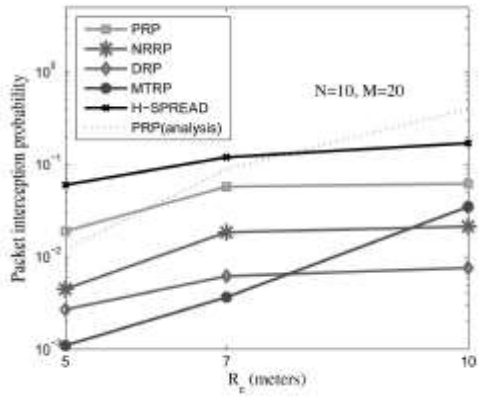

Fig.5: Packet interception probability versus Re.

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 route 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 (i.e., 0:01 ≤ PS ≤ 0:1). This clearly demonstrates that the sample topologies used in our simulations are representative and sufficient, and Fig. 14. packet interception probability versus N. Fig. 15. Packet interception probability versus M. simulation results does represent the general performance trend. When the packet interception probability is high (PS > 0:1) or low (PS < 0:01), the gap between the theoretical and simulated results becomes more significant. The overly-optimistic behavior of the analytical model in the low PS regime is due to ignoring the boundary effect when modeling random propagation. The overly-pessimistic behavior in the high PS regime is due to the asymptotic assumption made in the analytical model, which understates the spatial separation between routes when node density is no high enough. We plot the packet interception probability as a function of the size of the black hole in Fig. 16. It is clear that the interception probability increases with Re. This trend is in line with our analytical results shown in Fig. 11.

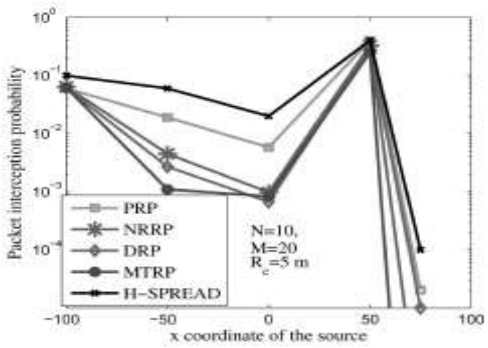

Fig. 6: Packet interception probability at different source location.

In Fig. 17, we study the impact of node connectivity. The number of nodes is changed from 1,000 to 3,000, corresponding to changing the average node connectivity degree from 8 to 24. It can be observed that, in general, the packet interception probabilities of the four proposed schemes do not change significantly with node connectivity. From Fig. 11, we can find that even for the asymptotic case, for which the average node degree is infinite, the theoretical interception probability of the PRP scheme is about 1×10^2, hitch is slightly smaller than the simulation results. Such insensitivity to the node connectivity/density is because the packet interception probability is mainly decided by how dispersive the shares can be geographically after random propagation, i.e., how large the concentered circles in Fig. 3 can be and how the shares are distributed over these circles. As long as the nodes are uniformly distributed, the change of node density does not impact the size of these circles, north distribution of the shares over these circles. In contrast, the packet interception probability of H-SPREAD decreases significantly with the increase in node density, because more node-disjoint routes can be found. In Fig. 18, we slide the x-coordinate of the source node along the line y ¼ 0 to evaluate the packet interception probabilities at different source locations in the network. A segmented trend can be observed: When the source is far away from the black hole ($-100 \leq x \leq 0$), the closer the source is to the black hole, the smaller the packet interception probability will be. This is in line with our analytical result in Fig. 12. Note that when x = -100 (this is at the boundary), the gap between the proposed schemes are small, because all shares can only be propagated to the right, making the random propagation process of PRP, DRP, and NRRP similar to that of MTRP. However, when the source is close to the black hole, i.e., x 0, the trend in interception probability is reversed. This is because more and more shares are intercepted during the propagation phase. When x ¼ 50, which corresponds to the scenario where the source is placed right at the center of the black hole, the interception probabilities reach their maximum value. After that, they decrease quickly as the source gets farther away from the black hole. In all segments, the packet interception probabilities of the DRP, NRRP, and MTRP schemes are smaller than that of H-SPREAD.

We evaluate the average number of hops of the end-to-end route as a function of the TTL value in Fig. 19. This hop count metric can be considered as an indirect t measurement of the energy efficiency of the routes generated by the Fig. 17. Packet interception probability versus number of nodes. Fig.16. Packet interception probability versus Re. Fig. 18. Packet interception probability at different source location. Fig. 19. Hop count of route versus N. routing schemes. It can be observed that the hop count under PRP, DRP, and NRRP increases linearly with N, while the hop count under MTRP only increases slowly with N. The TTL value N does not play a role in the H-SPREAD scheme. Under large N, e.g., when N ¼ 25, the randomized algorithm achieves better security performance than H-SPREAD. However, the hop count of H-SPREAD is about 1/3 of that of PRP, DRP, and NRRP, and about 1/2 of that of MTRP. The relatively large hop count in the randomized algorithms is the cost for stronger capability of bypassing black holes.

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 [15]. 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 [8], multipath DSR [5], and the AOMDV [13] and AODMV [24] algorithms that modify the AODV for multipath functionality. As pointed out in [24], 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 [11], [12] 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 [10] improves upon SPREAD by simultaneously accounting for both security and reliability requirements.

The work in [6], [7] 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 [23] considers the report fabrication attacks launched by compromised nodes. The work in [19] 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 [16], See MR [14], Burmester's approach [3], and AODV-MAP [21]. Among them, SRP uses end-to-end symmetric cryptography to protect the integrity of the route discovery; See MR protects against the denial-of-service attack from a bounded number of collaborate g 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.

Given a set of paths that have been constructed, the third type of work studies the optimal way of using these paths to maximize security. For example, the Secure Message Transmission (SMT) mechanism proposed in [17] continuously

updates the rating of the routes: For each successful (failed) share, the rating of the corresponding route is increased (decreased). The delivery of subsequent shares will be in favor of those routes with high ratings. The work in [4] studies two different ways of spreading an information packet into shares: secret sharing multipath aggregation (SMA) and dispersed (message-splitting) multipath aggregation (DMA). It shows SMA achieves better security at the cost of higher overhead, while the performance of DMA is exactly the complementary of SMA. To reduce unnecessary retransmissions and improve energy efficiency, the Gossiping algorithm [9] was proposed as a form of controlled flooding, whereby a node retransmits packets according to a reassigned probability.

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. 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 security enhanced dynamic routing could be used with cryptography-based system designs to further improve the security of data transmission over networks.

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 cut around- 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.

Acknowledgements

- My sincere thanks to our guide Mr. M. Srikanth yadav for the successful completion of this project.
- 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" canter.

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 Applications (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] 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 NFOCOM, 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.
[19] K. Ren, W. Lou, and Y. Zhang, "LEDS: Providing Location-Aware End-to-End Data Security in Wireless Sensor Networks," Proc. IEEE INFOCOM, 2006.
[20] D.R. Stinson, Cryptography, Theory and Practice. CRC Press, 2006.
[21] B. Vaidya, J.Y. Pyun, J.A. Park, and S.J. Han, "Secure Multipath Routing Scheme for Mobile Ad Hoc Network," Proc. IEEE Int'l Symp. Dependable, Autonomic and Secure Computing, pp. 163-171, 2007.
[22] A.D. Wood and J.A. Stankovic, "Denial of Service in Sensor Networks," Computer, vol. 35, no. 10, pp. 54-62, Oct. 2002.
[23] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, "Toward Resilient Security in Wireless Sensor Networks," Proc. ACM MobiHoc, 2005.
[24] Z. Ye, V. Krishnamurthy, and S.K. Tripathi, "A Framework for Reliable Routing in Mobile Ad Hoc Networks," Proc. IEEE INFOCOM, vol. 1, pp. 270-280, Mar. 2003.