Vol. 1, Issue 3, pp.1168-1174

Review on Secure data in Wireless Sensor Networks using Randomized multipath routing

[1]L.Kiran kumar, [2]V.Ranjith kumar

[1]Department of Computer Science & Information Technology, Jyothishmathi Institute of Tech & Sciences, JNTU, Hyderabad, AP, INDIA.

[2] Department of Computer Science & Information Technology, Jyothishmathi Institute of Tech & Sciences, JNTU, Hyderabad, AP, INDIA.

Abstract-
Security in wireless sensor networks (wsn) is major issue recent years i.e., data confidentiality, authenticity, denial of service. In this paper we present secure data delivery mechanism using security protocol. It can compute the same routes known to the source, hence, making all information sent over these routes vulnerable to its attacks. We develop mechanisms that generate randomized dispersive routes. In this paper data is splits and shares in packets send through different router using multipath routing technique like Aodv and Dsr protocols. 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. We use limited-flooding for retransmission probability for a packet at a sensor node. Providing end-to-end data security i.e., data confidentiality, authenticity and availability in wireless sensor networks. We evaluate the performance of our scheme using extensive simulate.

Index Terms—Randomized multipath routing, secure data delivery

1. INTRODUCTION

Wireless sensor networks (WSNs) have drawn a lot of attention recently due to their broad applications in both military and civilian operations. A WSN usually consists of a large number of ultra-small, low-cost devices that have limited energy resources, computation, memory, and communication capacities and for the applications such as battlefield reconnaissance and homeland security monitoring.

WSNs are often deployed in a vast terrain to detect events of interest and deliver data reports over multi-hop wireless paths to the sink. Data security is essential for these mission critical applications to work in unattended and even hostile environment.

Most of the security threats in WSNs are compromised node (CN) and denial of service (DOS). Compromised node (CN) could have multiple nodes to obtain their carried keying materials and control them, and thus is able to intercept data transmitted through these nodes thereafter. As the number of compromised nodes grows, communication links between uncompromised nodes and compromised nodes through malicious crypto analysis. Hence, this type of attacks could lead to data confidentiality in WSNs. denial of service (DOS) attack is any event that diminishes or eliminates a network's capacity to perform its expected function Hardware failures, software bugs, resource exhaustion, environmental conditions, or any complicated interaction between these factors can cause a DoS. Although attackers commonly use the Internet to exploit software bugs when making DoS attacks. These two WSNs attacks are similar in generating black holes.

A black hole is 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. In compromised node, 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. WSNs first the packet is broken into P shares using a(K,P) 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 P 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 (e.g., in-hop routes). The P shares are then distributed over these routes and delivered to the destination. As long as at least P-k+1 (or P) shares bypass the compromised nodes, the adversary cannot acquire the original packet

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 or jam all possible routes from the source to the destination, which is practically not possible.

2. RELATED WORK

Evaluation of Existing Security Designs in WSNs

In this section, we review existing security designs in the literature and evaluate them according to the above mentioned three data security requirements. We show that due to lack of end-to-end security guarantee, existing security designs fail to provide satisfactory security strength and are vulnerable to many types of attacks.

Limitations of existing key management schemes:

Symmetric secret key pre-distribution is viewed as the most practical approach for establishing secure channels among sensor nodes because of the resource limitations in WSNs. In the past few years, many secret key pre-distribution schemes have been proposed. By leveraging preloaded keying materials on each sensor node, these schemes establish pair wise keys between every two neighbor nodes after network deployment, and thus realize a hop-by-hop security paradigm. The security strength of these schemes is analyzed in term of the ratio of compromised communication links over total network communication links due to node compromise. Two types of node compromise are considered: random node capture and selective node capture, which differ in the key distribution information available to the attacker. Then to compromise the whole network communication, the attacker has to capture at least several hundreds of sensor nodes even under selective node capture attacks.

However, all these schemes assume a uniform wireless communication pattern in WSNs. Therefore, they are highly vulnerable to communication pattern oriented node capture attacks, because data of interest in WSNs are usually generated from the event happening area and transmitted all the way to the sink. Data confidentiality can be easily compromised due to lack of end-to-end security guarantee, since compromising any intermediate node will lead to the disclosure of the transmitted data. Therefore, the attacker only needs to compromise a relatively very small number of nodes to be able to obtain all the data transmitted in the whole network. According to the observed communication pattern and network topology. The inherent reason is that the hop-by-hop security paradigm can only protect local communications but fails to provide strong protection to the most valuable node-to-sink data, which is of more interest to the attacker. At the same time, as the attacker could decrypt the intercepted data, it could, therefore, freely manipulate them to deceive the sink and hence severely affect data availability. The lack of end-to end security association also makes it hard, if not impossible, to enforce data authenticity.

DATA SECURITY REQUIREMENTIN WSNs

The requirements of data security in WSNs are basically the same as those well defined in the traditional networks, that is, data confidentiality, authenticity and availability Data should be accessible only to authorized entities (usually the sink in WSNs), should be genuine, and should be always available upon request to the authorized entities. More specifically, the above three requirements can be further elaborated in WSNs as follows:

Data Confidentiality: In WSNs, data of interest usually appear as event reports sent by the sensing nodes from the area of occurrence via multihop paths to the sink. As the communication Range of sensor nodes is limited, the reports will be relayed by the intermediate nodes before finally reaching the sink. Hence, the requirement on data confidentiality In WSNs is naturally: as long as the event sensing nodes are not compromised, the confidentiality of the corresponding data report should not be compromised due to any other nodes' compromise including the intermediate nodes along the report forwarding route.

Data Authenticity: Data reports collected by WSNs are usually sensitive and even critical such as in military applications, and hence, it is important to ensure data authenticity in addition to confidentiality. Since the undetected compromised node(s) can always send false reports, cryptography alone can not fully prevent such attacks. However, if we require that a valid report be collectively endorsed by a number, says P (P > 1), of sensor nodes which sense the event at the same time, we can protect data authenticity to the extent that no less than P compromised nodes can forge a valid report. Furthermore, by exploiting the static and location aware nature of WSNs, we can require that a legitimate event report corresponding to certain area be only generated by the collaborative endorsement of no less than P nodes of that area. That is, to generate a valid report on a non-existing event happening in a certain area, the only way is to compromise P nodes in that area.

Data Availability: Since node compromise is usually inevitable in large-scale WSNs, it is rather important to prevent or be tolerant of the interference from compromised nodes as much as possible to ensure data availability. Therefore, security designs should be highly resilient to node compromise and the resulting attacks such as report disruption and selective forwarding attacks. In-network security-related processing such as false data filtering is vital to save scarce network resources and to prolong network lifetime.

3. SPLIT AND RANDOMIZED DISPERSIVE MULTIPATH ROUTING

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.

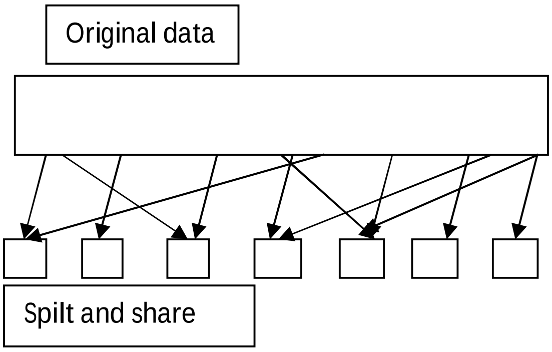


Fig-1 secure sharing phase

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 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.

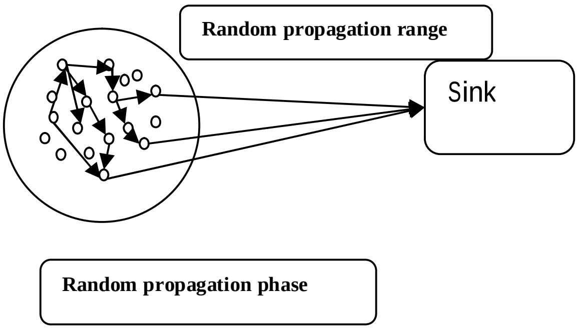


Fig-2: Randomized dispersive routing

4. RANDOMIZED RELIABLE MULTIPATH DELIVERY

I. Overview

As illustrated in Fig. 1, 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 destination, it first breaks the packet into P shares, according to a (p, k)-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 PPL field, whose initial value is set by the source node to control the total number of random relays. After each relay, the PPL field is reduced by 1. When the PPL 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 P shares, it can reconstruct the original packet. No information can be recovered from less than P shares.

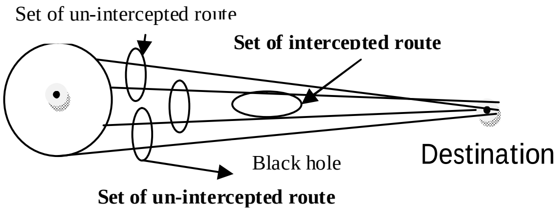


Fig -3 Implication of route depressiveness on bypassing the black hole

The effect of route depressiveness on bypassing black holes is illustrated in Fig. 3, 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.

II. Random Share Allocation

The second issue is how to select the paths, how to choose an appropriate value of (*T*, *N*), and how to allocate the shares onto each selected path such that the maximum security can be achieved. We consider the case that a message is compromised due to compromised nodes. We assume that if a node is compromised, all the credentials of that node will be compromised. So the message shares traveling through that node are all intercepted and recovered. Given the available independent paths and their corresponding security characteristics, the fundamental objective is to maximize the security by allocating the shares in such a way that the adversary has to compromise all the paths to recover the message. The simplest and most intuitive share allocation scheme is to choose *N* as the number of available paths, apply (*N*,*N*) secret sharing, and allocate one share onto each path. This will achieve the desired maximum security with least processing cost. However, in an ad hoc network, wireless links are instable and the topology changes frequently. Sometimes packets might be dropped due to the bad wireless channel condition, the collision at MAC layer transmission, or stale routing information.

In the case that packet loss does occur, this type of non-redundant share allocation will disable the reconstruction of the message at the intended destination. To deal with this problem, it is usually necessary to introduce some redundancy (i.e. $P<K$) in the split multipath scheme to improve the reliability, i.e. the destination would have better chance to receive enough shares for reconstructing the message. Generally speaking, security and reliability are two contradictive design goals - more redundancy implies better reliability but worse security. However, due to the salient feature of the threshold secret sharing, we develop the redundant split multipath feature of the threshold secret sharing, we develop the redundant split multipath share allocation which could tolerate certain packet losses while at the same time maintain the maximum security, i.e. forcing the adversary to compromise all the paths to compromise the message.

We formulate the share allocation into a constrained optimization problem, with the objective to minimize the message compromise probability. Our investigation to the optimal share allocation reveals that, by choosing an appropriate (P, K) value and allocating the shares onto each path carefully, we could improve the reliability by tolerating certain packet loss without sacrificing the security. The maximum redundancy we can add to the split multipath scheme without sacrificing security is identified. The optimal share allocation is proposed share allocation which could tolerate certain packet losses while at the same time maintain the maximum security, i.e. forcing the adversary to compromise all the paths to compromise the message. We formulate the share allocation into a constrained optimization problem, with the objective to minimize the message compromise probability. our investigation to the optimal share allocation reveals that, by choosing an appropriate (*P*,*K*) value and allocating the shares onto each path carefully, we could improve the reliability by tolerating certain packet loss without sacrificing the security. The maximum redundancy we can add to the split multipath routing without sacrificing security is identified.

5 SECURITY ANALYSIS

Security analysis in our case must be done with respect to the number of node compromises. Three fundamental questions arise:

1. How many compromised nodes does an attacker need at best to eavesdrop successfully and break confidentiality for a given scheme? Also, which nodes should be attacked?
2. What is the minimal number of nodes an attacker needs to compromise to inject false data into the network? Which nodes should be chosen?
3. How many nodes must be compromised in order for an attacker to succeed in a DoS attack?

It is important to underline that an attacker might not have the choice of which nodes to compromise. In practice, if *n* nodes need to be compromised for an attack to succeed, the attacker may not have access to all of these *n* nodes. Also, if the attacker does not have full knowledge of the topology, it may also be difficult to guess the interesting nodes to compromise. It may be a requirement that an attacker needs to compromise more nodes than the theoretical threshold.

A. Denial of service attacks

There are two types of DoS attacks: those where attackers stop emitting data (let us call it no-data DoS attacks) and those where they send garbage data (let us call it garbage data DoS attacks). Note that no-data DoS attacks include the case where there is no attacker, but a sensor node simply goes down (e.g., because it runs out of battery power.) Garbage data DoS attacks are more difficult to handle. In the absence of data authentication, an attacker needs only to one path and send some garbage data on it. In this case, the sink has multiple possible outputs for but cannot tell which ones are valid. In the presence of data authentication, garbage-data DoS attacks are indistinguishable from no-data DoS attacks – invalid reconstructions are rejected as if the share had never arrived. No-data and garbage-data DoS attack in the presence of need to prevent the sink from gathering *t* valid shares. Therefore, an attacker needs to compromise at least p-k+1 distinct paths, i.e., in the worst case, p-k+1 nodes. If the attacker does not know the routing topology, it cannot do anything but compromise random nodes. Therefore, it will probably have to compromise more than p-k+1 node.

Let *te* and *td* be, respectively, the minimum number of compromised nodes required to eavesdrop communications and the minimum number of compromised nodes required to succeed in a DoS attack. From previous sections, *te* = *t* and *td* = p-k+1. Note that the higher *te*, the lower *td*. One can make a trade-off by choosing $t \approx p+1/2$. Any higher values would give better resistance to eavesdropping whereas any lower values will give better resistance to DoS attacks

B. 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. As shown in Fig. 3, 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,

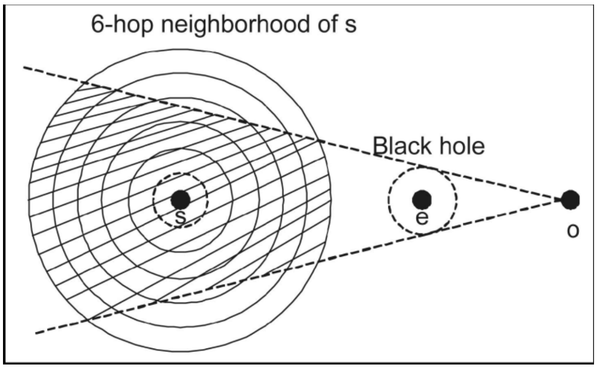
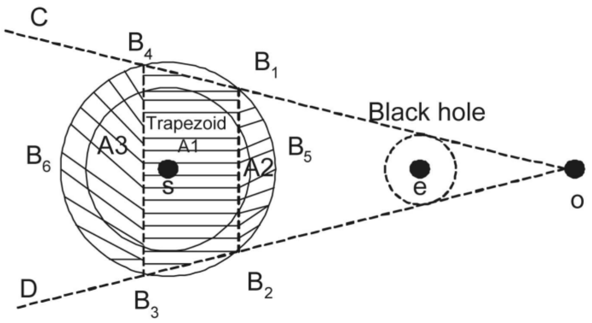


Fig. 3. Packet interception area, a six-hop random propagation example

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 o 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 {1 ...N}. 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 in-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 o 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. The interception probability for an arbitrary share of information is given by

$$P_I = \sum_{i=1}^{N} Pr\{\varepsilon = i\} \frac{s_i}{Area\ of\ ring\ i} \qquad (1)$$

$$\sum_{i=1}^{N} Pr\{\varepsilon = i\} \frac{s_i}{\pi R^2 - \pi(i-1)^2 R_h^2} \qquad (2)$$

Accordingly, the worst-case probability that at least K out of P shares are intercepted by E is given by

$$P_s^{max} = \sum_{K=T}^{M} \binom{M}{K} P_I^K (-P_I)^{M-k}$$

C. Derivation of the Packet Interception Area

The derivation of Si falls into one of the following three cases

Case 1: when $iR_h \leq \frac{R_g d_g}{d_g}$ring *i* is completely covered by the shaded region. Therefore,

$$s_i^{(case1)} = \pi[i^2 - (i-1)^2]R_h^2 1 \leq i \leq \frac{Reds}{rede}.$$

(3)

Case2: when (i-1 $R_h \leq \frac{R_g d_g}{d_g} < iR_h$,as show in fig 4 ring *i* is partially shaded. The shaded area of ring i is the intersection of circle i and the cone CoD minus the area of Circle$i-1$. The area of this intersection is composed of three components: the trapezoid A1 (B1B2B3B4), two circles

Segments A2 (surrounded by arch B1B5B2 and chord B1B2), and A3 (surrounded by arch B3B6B4 and chord B3B4). It can be shown that A1 has a height $h_A = x_1 - x_2$, where

$$x_1 \overset{\text{def}}{\equiv} \frac{R_g^2 d_s + \sqrt{R_g^4 d_s^2 - d_g^2 R_g^2 d_s^2 + d_g^4 i^2 R_h^2 - i^2 d_g^2 R_h^2 R_g^2}}{d_g^3}, \qquad (4)$$

$$x_2 \overset{\text{def}}{\equiv} \frac{R_g^2 d_s + \sqrt{R_g^4 d_s^2 - d_g^2 R_g^2 d_s^2 + d_g^4 i^2 R_h^2 - i^2 d_g^2 R_h^2 R_g^2}}{}, \qquad (5)$$

he lengths of the two parallel edges of A1 are given by

$$l_1 = 2\left(-\frac{R_g}{\sqrt{d_g^2 - R_g^2}} x_1 + \frac{R_g d_s}{\sqrt{d_g^2 - R_g^2}} \right), \qquad (6)$$

$$l_2 = 2\left(-\frac{R_g}{\sqrt{d_g^2 - R_g^2}} x_1 + \frac{R_g d_s}{\sqrt{d_g^2 - R_g^2}} \right) \qquad (7)$$

Therefore, the area of A1 is given by

$$s_1^{(A_1)} = \frac{(l1 + l2) h_{A_1}}{2} \qquad (8)$$

The area of A2 and A3 are given by

$$s_i^{(A2)} = (R_h)^2 arctan\left(\frac{0.5 l_1}{x_1}\right) - 0.5 x_1 l_1 \qquad (9)$$

$$s_i^{(A3)} = (R_h)^2 arctan\left(\frac{0.5 l_2}{x_2}\right) - 0.5 x_1 l_1 \qquad (10)$$

So the total shaded area in ring i, $\left[\frac{R_g d_g}{R_h d_g}\right] \leq i \leq \left[\frac{R_g d_g}{R_g d_g} + 1\right]$, given by

$$s_i^{(case\ 2)} = s_i^{A_1} + s_i^{A_2} + s_i^{(A_3)} - \pi(i-1)^2 R_h^2. \qquad (11)$$

6 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.

REFERENCES

[1] P.C. Lee, V. Misra, and D. Rubenstein, Distributed Algorithms for Secure Multipath Routing in Attack-Resistant Networks," EEE/ ACM Trans. Networking, vol. 15, no. 6, pp. 1490-1501, Dec. 2007.

[2] 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

[3] 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.

[4] K. Ren, W. Lou, and Y. Zhang, "LEDS: Providing Location-Aware End-to-End Data Security in Wireless Sensor Networks," Proc. IEEE INFOCOM, 2006.

[5] A.D. Wood and J.A. Stankovic, "Denial of Service in Sensor Networks," Computer, vol. 35, no. 10, pp. 54-62, Oct. 2002.