Volume 3, Issue 11, November 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Survey on Protected data Transmission on Wireless Sensor Networks using Dispersive Routes

Shanthi D L
Assistant professor, Department of ISE, BMSIT,
Bangalore, Karnataka, India

Abstract: Wireless Sensor Networks (WSN) are rising as new stage in the IT ecosystem and in rich field of active research involving hardware and system design, distributed algorithms, networking ,security and social factors. Security is a term used about the characteristics of integrity, authentication, privacy, anti-playback, and nonrepudiation attacks against wireless sensor networks. Of the various possible security threats encountered in a wireless sensor network (WSN), this paper is specifically concerned in fighting against two types of attacks: compromised node (CN) and denial of service (DOS), which generates black holes. General classic multipath routing methods are vulnerable to these attacks, due to their deterministic nature. So once the opponent acquires the routing algorithm, it can figure out the same routes known to the source, making all information sent over these routes vulnerable to attacks. The proposed paper, develop mechanisms that generate randomized multipath routes. Under this approach, the paths taken by the "shares" of different packets change over time. So even if the algorithm becomes known to the adversary, the adversary still cannot locate the routes traversed by each packet. Besides arbitrariness, the routes are also highly dispersive and energy efficient. We analytically investigate the security and energy performance of the proposed schemes. Simulations are conducted to verify the validity of our mechanisms.

Keywords: - Wireless sensor networks, secure data delivery, Randomized multi-path routing

I. INTRODUCTION

Recent advancements in technology and highly integrated digital electronics have led to the development of micro sensors. These sensors are generally equipped with processing, storing and communication capabilities. Sensors measures the characteristics and atmosphere of the ecosystem [1][2][3].The main task of a wireless sensor node is to sense and collect data from a province, process and transmit it to the base station or sink node where the application lies. Since many network applications require hundreds or thousands of sensor nodes, often installed in remote and inaccessible areas. The routing of incoming data and routing protocol is an important factor in designing communication in WSNs.

The challenging task of routing in sensor network has several characteristics that distinguish from the existing communication and wireless ad-hoc networks [1].

1. It is not possible to build a global addressing scheme for sensor nodes.
2. Requires the flow of sensed data from multiple sources to a particular sink.
3. Redundancy in traffic.
4. Nodes are constrained by means of transmission power, energy, and storage.

II. BASIC SECURITY SCHEMES IN WSNS

The applications for WSNs are many and diverse; typically involve some kind of, tracking, monitoring and controlling, smart buildings, transportation, space exploration, disaster detection. In order to operate these applications correctly, it is necessary to maintain confidentiality and security of the transmitted data.

Security is a broadly used term encompassing the characteristics of authentication, reliability, isolation, nonrepudiation, and anti-playback [4]. The techniques like cryptography, steganography, Physical Layer Secure Access are used to provide the security to sensor networks.

A. Cryptography

The encryption-decryption techniques developed for the traditional wired networks are not practical to be applied directly for wireless sensor networks. WSNs consist of sensors nodes which really suffer from the lack of resources [5][6][7]. Applying the security mechanisms such as encryption could also raise delay, jitter and packet loss in wireless sensor networks [8].

B. Steganography

The objective of steganography is to modify the carrier in a way that is not traceable. It hides the existence of the concealed channel and also, in the case that we want to send a secret data without sender information or when we want to distribute secret data publicly. However, securing wireless sensor networks is not directly related to steganography and processing multimedia data (like audio, video) with the poor resources [9] of the sensors.

C. Physical layer secure access

Physical layer secure access in wireless sensor networks could be provided by using frequency hopping. A scheme as proposed in [10] could also be utilized which introduces secure physical layer access employing the singular vectors with the channel synthesized modulation.

III. SECURITY ATTACKS IN WSNS

Most of the security attacks in wireless sensor networks are similar to wired networks. But, Because of unattended nature of WSNs, are the candidates for various classes of attacks, some of them are stated here.

A. Denial of service

Any event that reduces or eliminates a networks capacity to perform its expected function. Reasons may be hardware failures, software viruses, resource collapse, ecological conditions or other complicated interactions. The mechanisms to prevent DoS attacks include payment for network resources, strong verification and identification of traffic [11].

B. Compromised node attack

It is a critical security requirement for the successful deployment of large-scale wireless sensor networks. A node compromise attack often consists of the following stages:

- Physically obtaining and conceding the sensors.
- Redistributing the negotiated nodes back to the sensor network.
- Compromised sensors respond the network by inducting attacks.

C. Sybil attack

A node can pretend to be more than one node using the identities of other true nodes. This type of attack where a node falsifies the identities of more than one node is the Sybil attack [12]. Sybil attack tries to degrade the truthfulness of data, security and resource consumption that the distributed algorithm attempts to achieve. This can be made for attacking the distributed storage, routing mechanism, data accumulation, impartial resource allocation [13].

D. Black hole/sinkhole attack

A malicious node acts as a black hole [1] to attract all the traffic in the sensor network. Especially in a flooding based protocol, the rival listens to needs for routes then replies to the target nodes that it contains the high quality or shortest path to the base station. Once the wicked device is been able to insert itself between the interactive nodes, can do anything with the packets passing between them.

IV. MOTIVATIONS

Of the various possible security threats encountered in a wireless sensor network (WSN), this paper is specifically concerned in fighting against two types of attacks: compromised node (CN) and denial of service (DOS) [11]. As mentioned, the CN attack, an adversary physically compromises a subset of nodes to snoop information, whereas in the DOS attack, the opponent interferes with the normal operation of the network by dynamically disturbing, altering, or even paralyzing the functionality of a subset of nodes. Due to the unattended nature of WSNs, adversaries can easily produce black holes. Severe CN and DOS attacks can disrupt normal data delivery between sensor nodes and the sink. A conventional cryptography-based security method cannot alone provide satisfactory solutions to these problems. This is because, once a node is cooperated, the challenger can always acquire the encryption/decryption keys of that node, and thus can capture any information delivered through it. Likewise, an opponent can always perform DOS attacks (e.g., jamming) even if it does not have any knowledge of the underlying cryptosystem. One curative solution to these attacks is to exploit the network's routing functionality. Precisely, if the locations of the black holes are known in advance, then data can be delivered over paths that avoid these holes, whenever possible. In practice, due to the effort of attaining such location statistics, the above notion is implemented in a probabilistic way, characteristically through a two-step process.

1. The packet is broken into M shares (i.e., a packet carries partial information) using a threshold secret sharing mechanism such as the Shamir's algorithm [14][19]. The original information can be recovered from a combination of at least T shares, but no information can be estimated from less than T shares.
2. Multiple routes from the source to the destination are computed according to some multipath routing algorithms [15][16]. These routes are node-disjoint and 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 the original packet.

The three security problems exist in the above mentioned counter attack approach:

1. Due to the deterministic nature of multipath routing algorithm the adversary can compromise selectively or jam nodes.
2. When node density is moderate and source and destination nodes are several hops apart then very few node-disjoint routes [17] can be found, which will demoralizes the security performance of multipath approach.
3. The routes may not be spatially dispersive enough to avoid a moderate-sized black hole based on the constraints imposed.

V. PROPOSED SYSTEM

Our proposed solution is to establish a randomized multi-path routing algorithm that can overcome the black holes formed by CN and DoS attacks. Instead of selecting paths from pre-computed routes, our objective is to work out multiple paths in a randomized way. Each time an data packet needs to be sent, the routes taken by various shares of different packets keep varying over time. As a result, a large number of routes can be potentially generated for each source and destination. To capture different packets, the adversary has to compromise or jam all possible routes from the source to the destination, which is nearly infeasible.

A. Advantages

- Provides highly dispersive random routes at low energy cost. Unlike in Wanderer Scheme [18] which leads to long paths, consuming high energy.
- If the routing algorithm becomes known to the adversary, the adversary still cannot identify the routes traversed by each packet.
- Experiences a small amount of communication overhead

B. Randomized multipath delivery

Overview

For secure information delivery in a WSN we consider a three-phase approach:

- Secret sharing of information
- Randomized communication of each information share
- Normal routing (e.g., min-hop routing) toward the sink

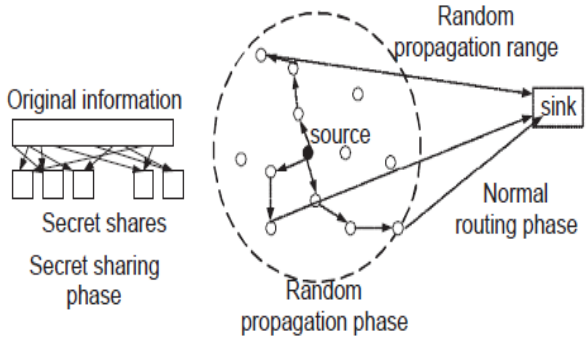

Figure 1 . Randomized Routing in WSN

In detail, when a sensor node wants to send a packet to the sink, it breakdowns the packet into M shares, according to a (T, M) -threshold secret sharing algorithm [14][19]. Each share is then transmitted to some randomly nominated neighbor. That neighbor will continue to transfer the share it has received to other randomly selected neighbors, and so on. In each share, there is a Time To Live (TTL) field, whose first value is set by the source node to control the total number of random transmits. After each relay, the TTL field is decreased by1. 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 rebuild the original packet. No information can be mended from less than T shares.

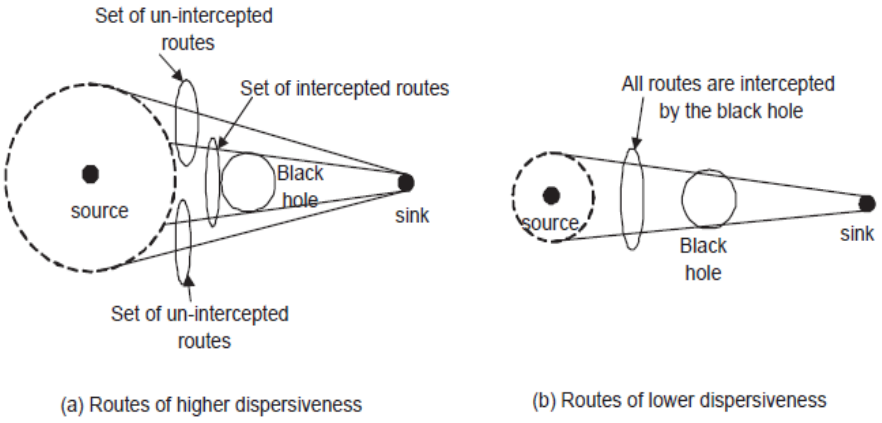

Figure 2. Implication of route depressiveness on by passing the black hole.

The outcome of route depressiveness on bypassing black holes is illustrated in Figure 2. A bigger dotted circle implies that the resulting routes are geographically more dispersive. Relating the two cases in Figure 2, it is clear that the routes of higher depressiveness are more capable of circumventing the black hole. Noticeably, the random propagation phase is the key component that dictates the security and energy performance of the entire mechanism.

C. Random propagation of information shares

To vary routes, an ideal random propagation approach, that would propagate shares depressively as much as possible, i.e., propagating the shares farther from their source and towards the sink. At the similar time, it is highly desirable to have an energy efficient transmission, which calls for limiting the number of arbitrarily propagated hops. Now the challenge here lies in the random and distributed nature of the propagation i.e. a share may be sent one hop farther from its source in a given step, but may be sent back nearer to the source in the next step, wasting both steps from a security point of view. The confrontation is, some control needs to be enforced on the random propagation process.

Generally there are four types of schemes:

1. Purely Random Propagation: It utilizes only one-hop neighbourhood information and provides baseline performance.
2. Non-repetitive random Propagation: Records all traversed nodes to avoid traversing them again in the future.
3. Directed Random Propagation: It utilizes two-hop neighbourhood information to improve the propagation efficiency, leading to a smaller packet capture probability.
4. Multicast Tree-Assisted Random Propagation: It tries to propagate shares in the route of the sink, making the delivery process more energy efficient.

D. Analysis of the PRP scheme

D. A .Network and Attack Models

We consider an area S that is uniformly covered by sensors with density ρ. We assume a unit-disk model for the sensor communication, i.e., the pass on signal from a sensor can be successfully received by any sensor that is at most Rh meters away. Multihop relay is used if the intended destination is more than Rh away from the source.

The following are the assumptions made:

- Under link-level security established using a conventional cryptography; a node cannot decrypt a cipher text overheard over the wireless channel if it is not the intended receiver.
- A link key is harmless unless the opponent actually compromises either side of the link.
- The adversary cannot negotiate the sink and its immediate surrounding nodes, sink neighbor nodes can be physically secured by the network operator [5][20].
- The black hole formed by the compromised nodes can be approximated by its circumcircle, i.e., the lowest circle that covers the shape of the black hole.
- Note that the operation does not depend on the shape of the black hole. We denote the circle, its center, and its radius by E, e, and Re, respectively.
- We also assume the area S is suitably large.
- The WSNs operations, any end-to-end path that traverses through this circle is considered to be vulnerable to the attacks.

D.B. Security definition for packet capture area

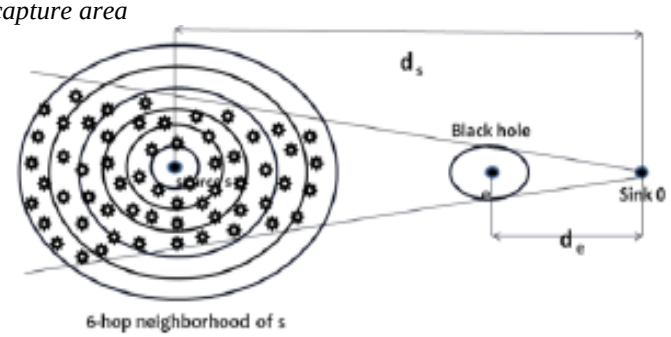

Figure3 . A 6-hop random propagation example

For a given source node, the security provided by the protocol is defined as the worst-case probability that for the M shares of an information packet sent from the source, at least T of them are interrupted 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 + 1 circles co-centered at s (Figure3). For the i^{th} circle, $1 \leq i \leq N$, the radius is iRh. For circle 0, its radius is 0. These N + 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 transmission phase, the id of the ring in which the last acceptance node, say w, is located is a discrete random variable ξ with state space {1,…, N}. The actual path from w to the sink is decided by the specific routing protocol employed by the network. However, the route given by min-hop routing, which under high node density can be estimated by the line between w and the sink, gives an upper bound on the packet interruption rates under all other routing protocols.

The worst-case scenario for packet interruption happens when the points s, e, and o, (see Figure 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 reaches its maximum area, and thus gives the maximum packet interruption 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

$$P_I = \sum_{i=1}^{N} \Pr\{\xi = i\} \frac{S_i}{\text{Area of ring } i} = \sum_{i=1}^{N} \Pr\{\xi = i\} \frac{S_i}{\pi i^2 R_h^2 - \pi(i-1)^2 R_h^2}. \quad (1)$$

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

$$P_S^{(\max)} = \sum_{k=T}^{M} \binom{M}{k} P_I^k (1 - P_I)^{M-k} \quad (2)$$

D.C. Analysis of Black hole interception area

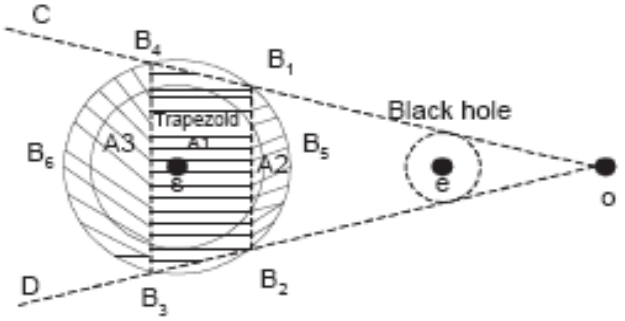

Figure 4 Packet interception area case 2

The derivation of Si falls into one of the following 3 cases:

Case 1: When $iR_h \le \frac{R_e d_s}{d_e}$ (e.g., rings 1 to 3 in Figure 3), ring i is completely covered by the shaded region. Therefore,

$$S_i^{(case\ 1)} = \pi[i^2 - (i-1)^2]R_h^2, 1 \le i \le \left\lfloor \frac{R_e d_s}{R_h d_e} \right\rfloor \quad (3)$$

Case 2: When (i-1) $R_h < \frac{R_e d_s}{d_e} < iR_h$, as shown in Figure 4, ring i is partially shaded. The shaded area of ring I is the intersection of circle I and the cone C o D minus the area of circle i-1. The area of this intersection is composed of three components: The trapezoid A_1 (B_1,B_2 ,B_3,B_4), two circle segments A_2 (surrounded by arch B_1 B_5B_2 and chord B_1B_2), and A_3 (surrounded by arch $B_3B_6B_4$ and chord B_3B_4). It can be shown that A_1 has a height h_{A1} = x1-x2 where

$$x_1 \triangleq \frac{R_e^2 d_s + \sqrt{R_e^4 d_s^2 - d_e^2 R_2^2 d_s^2 + d_e^4 i^2 R_h^2 - i^2 d_e^2 R_h^2 R_e^2}}{d_e^2} \quad (4)$$

$$x_2 \triangleq \frac{R_e^2 d_s - \sqrt{R_e^4 d_s^2 - d_e^2 R_2^2 d_s^2 + d_e^4 i^2 R_h^2 - i^2 d_e^2 R_h^2 R_e^2}}{d_e^2}. \quad (5)$$

The lengths of the two parallel edges of A_1 are given by

$$l_1 = 2\left(-\frac{R_e}{\sqrt{d_e^2 - R_e^2}} x_1 + \frac{R_e d_s}{\sqrt{d_e^2 - R_e^2}}\right) \quad (6)$$

$$l_2 = 2\left(-\frac{R_e}{\sqrt{d_e^2 - R_e^2}} x_2 + \frac{R_e d_s}{\sqrt{d_e^2 - R_e^2}}\right). \quad (7)$$

Therefore, the area of A_1 is given by

$$S_i^{(A_1)} = \frac{(l_1 + l_2)h_{A_1}}{2}. \quad (8)$$

The area of A_2 and A_3 are given by

$$S_i^{(A_2)} = (iR_h)^2 \arctan\left(\frac{0.5l_1}{x_1}\right) - 0.5x_1 l_1 \quad (9)$$

$$S_i^{(A_3)} = (iR_h)^2 \arctan\left(-\frac{0.5l_2}{x_2}\right) + 0.5x_2 l_2. \quad (10)$$

So the total shaded area in ring i, $\left\lceil \frac{R_e d_s}{R_h d_e} \right\rceil \le i \le \left\lfloor \frac{R_e d_s}{R_h d_e} + 1 \right\rfloor$, is given by

$$S_i^{(case\ 2)} = S_i^{(A_1)} + S_i^{(A_2)} + S_i^{(A_3)} - \pi(i-1)^2 R_h^2, \quad (11)$$

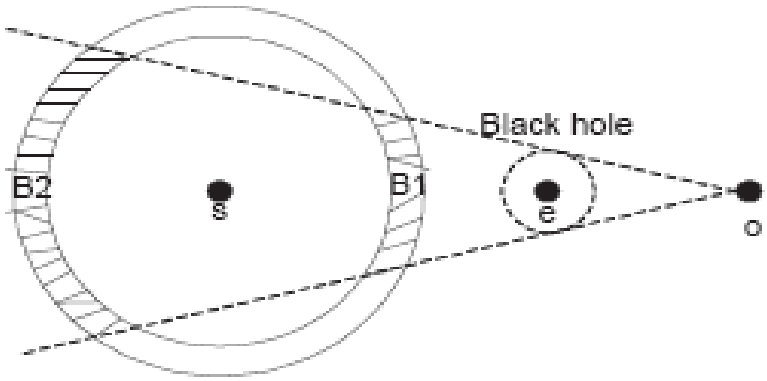

Figure 5 Packet-interception area: case 3

Case 3: When (i-1) $R_h >= \frac{R_e d_s}{d_e}$ as shown in Figure 5, ring i the shaded area in ring I is the sum of the areas of two ring segments $B_1$and B_2. Following a similar approach to case 2, the areas of B_1 and B_2 are approximated by

$$S_i^{(B_1)} \approx [i^2 - (i-1)^2] R_h^2 \arctan\left(\frac{0.5l_1}{x_1}\right) \quad (12)$$

$$S_i^{(B_2)} \approx [i^2 - (i-1)^2] R_h^2 \arctan\left(-\frac{0.5l_2}{x_2}\right) \quad (13)$$

where x_1, x_2, l_1, and l_2 are given by (4) through (7), with i referring to the ring being calculated. So the total shaded area in ring i is

$$S_i^{(case\ 3)} = S_i^{(B_1)} + S_i^{(B_2)}, \quad i \geq \left\lceil \frac{R_e d_s}{R_h d_e} + 1 \right\rceil \quad (14)$$

D.D. 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 arbitrary route consists of two elements. The first is a fixed N-hop component attributed to the random propagation operation. The second component involves sending the share from the last random relay node, i.e., w, to the sink o using a normal single path routing. Under the asymptotic notion, 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. This ratio can be calculated as follows. Suppose w is located in the ith ring. Let the distance between w and s be . (i-1)Rh ≤d≤iRh

Given that the angle between sw and so be θ, the distance between w and o is given by

$$d_{wo}^{(i)}(d,\theta) = \sqrt{d^2 + d_s^2 - 2dd_s\cos\theta} \quad (15)$$

D.E. Optimal Secret Sharing and Random Propagation

To obtain the maximum protection of the information, the verge parameter should be set as T = M. Then, increasing the number of propagation steps (N) and increasing the number of shares a packet is broken into (M) has a similar effect on reducing the message interception probability. Specifically, to achieve a given Ps(max) for a packet, either break the packet into more shares but limit the random propagation of these shares within a smaller range, or break the packet into smaller number shares but randomly propagate these shares into a larger range.

$$\begin{aligned} \text{minimize} \quad & Q^{(\text{PRP})}(M,N) \\ s.t. \quad & P_s^{(\max)}(M,N) \leq P_S^{(req)} \\ & 1 \leq M \leq M_{\max} \\ & 1 \leq N \leq N_{\max} \end{aligned} \quad (16)$$

Where M and N are variables and Ps (req) is the given security requirement. The upper bounds, Mmax and Nmax, are dictated by practical considerations such as the hardware or energy constraints.

E. System Design

S/w and H/w requirements

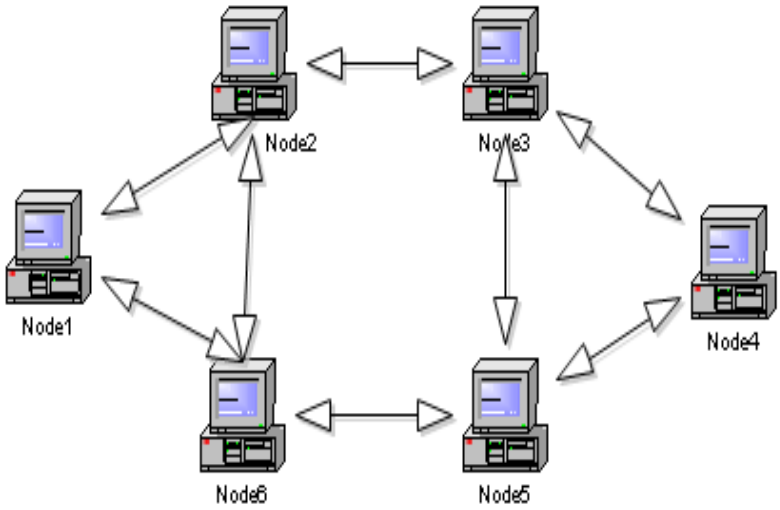

Figure 6: A System with 6 nodes

- Java1.6
- Java Swing – front end
- RMI-Remote Method
- Networking-Socket programming
- Java Serialization (using files) –Back end
- NS2-Simulator
- 10GB HDD(min)
- 128 MB RAM(min)
- Pentium P4 Processor 2.8Ghz(min)
- Windows98 or higher-Operating System

VI CONCLUSIONS

By analyzing and simulating the results have shown the effectiveness of the randomized dispersive routing in combating CN and DOS assaults. By appropriately setting the secret sharing and propagation parameters, the packet interception probability can be easily reduced by the new algorithms which are at least one order of magnitude smaller than approaches that use deterministic node-disjoint multipath routing. At the same time, we have also shown that this improved security performance comes at a reasonable cost of energy. Specifically, the energy depletion of the proposed randomized multipath routing algorithms is only one to two times higher than that of their deterministic counter-parts. The proposed algorithms can be applied to selective packets in WSNs to provide additional security levels.

REFERENCES

[1] kemal Akkaya and Mohamed Younis. A Survey on Routing Protocols for Wireless Sensor Networks *.Ad Hoc Networks. 200,3, 325-349.*

[2] I. F. Akyildiz et al., "Wireless Sensor networks : a Survey", *Computer Networks*, Vol. 38, PP 393-422, March 2002.

[3] Culler, D. E and Hong, W., "Wireless Sensor Networks", Communication of the ACM, Vol. 47, No. 6, June 2004, pp. 30-33.

[4] Karlof, C. and Wagner, D., "Secure routing in wireless sensor networks :Attacks and countermeasures", Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Network Applications and Protocols, September2003, pp. 293-315.

[5] Perrig, A., Szewczyk, R., Wen, V., Culler, D., and Tygar, J. D., "SPINS: Security Protocols for Sensor Networks", Wireless Networks, vol. 8, no.5, 2002, pp. 521-534.

[6] Jolly, G., Kuscu, M.C., Kokate, P., and Younis, M., "A Low-Energy Key Management Protocol for Wireless Sensor Networks", Proc. Eighth IEEE International Symposium on Computers and Communication, 2003. (ISCC 2003). vol.1, pp. 335 – 340 .

[7] Rabaey, J.M., Ammer, J., Karalar, T., Suetfei Li., Otis, B., Sheets, M.,and Tuan, T., "PicoRadios for wireless sensor networks: the next challenge in ultra-low power design" 2002 IEEE International Solid-State Circuits Conference (ISSCC 2002), Volume 1, 3-7 Feb. 2002, pp. 200 –201.

[8] Saleh, M. and Khatib, I. A., "Throughput Analysis of WEP Security in Ad Hoc Sensor Networks", Proc. The Second International Conference on Innovations in Information Technology (IIT'05), September 26-28, Dubai, 2005.

[9] Younis, M., Akkaya, K., Eltoweissy, M., and Wadaa, A., "On handling QoS traffic in wireless sensor networks", Proc. of the 37th Annual Hawaii International Conference on System Sciences, 2004, 5-8 January, 2004,pp. 292 – 301.

[10] Orihashi, M., Nakagawa, Y., Murakami, Y., and Kobayashi, K., "Channel synthesized modulation employing singular vector for secured access on physical layer", IEEE GLOBECOM 2003, Volume 3, 1-5 December, 2003, pp. 1226 – 1230.

[11] Anthony D. Wood, John A. Stankovic : "Denial of Service in Sensor Networks". In: IEEE Computer, Vol. 35, No.10, pp.54-62 (2002).

[12] S.Sharmila[1], G Umamaheswari[2]
"Detection Of Sybil Attack In Mobile Wireless Sensor Networks " International Journal Of Engineering Science & Advanced Technology Volume-2, Issue-2, 256 – 262,Mar-Apr 2012

[13] Newsome, J., Shi, E., Song, D, and Perrig, A, "The Sybil attack in sensornetworks: analysis & defences ", Proc. of the third internationalsymposium on Information processing in sensor networks, ACM, 2004, pp. 259 – 268.

[14] William Stallings. "Cryptography and network security"

[15] P. C. Lee, V. Misra, and D. Rubenstein. Distributed algorithms for secure multipath routing. In Proceedingsof *the IEEE INFOCOM Conference*, pages 1952–1963,Mar. 2005.

[16] P. C. Lee, V. Misra, and D. Rubenstein. Distributed algorithms for secure multipath routing in attack resistant networks .*IEEE/ACM Transactions on Networking*, 15(6):1490–1501, Dec. 2007.

[17] Z. Ye, V. Krishnamurthy, and S. K.Tripathi. A framework for reliable routing in mobile ad hoc networks. In *Proceedings of the IEEE INFOCOM Conference*, volume 1, pages 270–280, Mar. 2003.

[18] C. L. Barrett, S. J. Eidenbenz, L. Kroc, M. Marathe, and J. P. Smith."Parametric probabilistic sensor network routing. In *Proceedings ofthe ACM International Conference on Wireless Sensor Networks and Applications (WSNA)*, pages 122–131, 2003.

[19] D. R. Stinson. *Cryptography, Theory and Practice*.CRC Press, 2006.

[20] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh. Toward resilient security in wireless sensor networks. In *Proceedings of the ACM MobiHoc Conference*, 2005

