International Journal of Innovations & Advancement in Computer Science
IJIACS
ISSN 2347 – 8616
Volume 6, Issue 9
September 2017

An Efficient Mechanism to Embed Security and Congestion Control using Randomized Dispersive Routing in Wireless Sensor Networks

[1] **Mr.N.Sainath**
Associate Professor
Department of CSE
St Martin's Engineering College

[2] **M.Ravi Kumar**
Professor
Department of CSE
JBREC,

[3]**Dr.U.Moulali**
Professor
Department of CSE
JBREC

[4]**Mr.A.Prakash**
Professor
Department of CSE
St Martin's Engineering College

ABSTRACT

Now a days traffic and the sensor network security has many challenges in the transmission of data in the network. The existing schemes consider homogeneous sensor networks which have poor performance and scalability. Due to many-to-one traffic pattern, sensors may communicate with small portion of its neighbors. Key management is the critical process in sensor nodes to secure the data. Most existing schemes establish shared keys for all the sensors no matter whether they are communicating or not. Hence it leads to large storage overhead. Another problem in sensor network is compromised node attack and denial of service attack which occurs because of its wireless nature. Existing multi path routing algorithms are vulnerable to these attacks. So once an adversary acquires the routing algorithm, it can compute the same routes known to the source, and hence endanger all information sent over these routes. If an adversary performs node compromise attack, they can easily get the encryption/ decryption keys used by that node and hence they can intercept the information easily.

In this paper we are proposing a key management scheme which only establishes shared keys with their communicating neighbor and a mechanism to generate randomized multipath routes for secure transmission of data to the sink.

Here we are adopting heterogeneous sensor networks and we are utilizing elliptic curve cryptography for efficient key management which is more efficient, scalable, and highly secure and reduces communication overhead. The routes generated by our mechanism are highly dispersive, energy efficient and making them quite capable of bypassing the back holes at low energy cost.

KEYWORDS

Wireless Sensor Network, Non-Repetitive random propagation (NRRP) and Multi cat tree assisted random propagation (MTRP)

1. INTRODUCTION

WIRELESS sensor networks have applications in many areas, such as military, homeland security, health care, environment, agriculture, manufacturing, and so on. In the past several years, sensor networks have been a very active research area. Most previous research efforts consider homogeneous sensor networks, where all sensor nodes have the same capabilities. However, a homogeneous ad hoc net-work suffers from poor fundamental limits and performance. Research has demonstrated its performance bottleneck both theoretically and through simulation experiments and test bed measurements. Several recent works studied Heterogeneous Sensor Networks (HSNs), where sensor nodes have different capabilities in terms of communication, computation, energy supply, storage space, reliability and other aspects.

Key management is an essential cryptographic primitive upon which other security primitives are built. Due to resource constraints, achieving such key agreement in wireless sensor networks is non-trivial. In Eschenauer and Gligor first present a key management scheme for sensor networks based on probabilistic key pre-distribution. Several other key pre-distribution schemes have been proposed. Probabilistic key pre-distribution is a promising scheme for key management in sensor networks. To ensure such a scheme works well, the probability that each sensor shares at least one key with a neighbor sensor (referred to as key-sharing probability) should be high.

The above discussion shows that many existing key management schemes require a large storage space for key pre-distribution and are not suitable for small sensor nodes. Of the various possible security threats

that may be experienced by a wireless sensor network (WSN), in this paper we are specifically interested in combating two types of attacks: the compromised-node (CN) attack and the denial-of-service (DOS) attack. The CN attack refers to the situation when an adversary physically compromises a subset of nodes to eavesdrop information, whereas in the DOS attack, the adversary interferes with the normal operation of the WSN by actively disrupting, changing, or even destroying the functionality of a subset of nodes in the system. These two attacks are similar in the sense that they both generate black holes: areas within which the adversary can either passively intercept or actively block information delivery. Due to the unattended nature of WSNs, adversaries can easily produce such black holes. Severe CN and DOS attacks can disrupt normal data delivery between sensor nodes and the sink, or even partition the topology. A conventional cryptography-based security method cannot alone provide satisfactory solutions to these problems. This is because, by definition, once a node is compromised, the adversary can always acquire the encryption/decryption keys of that node, and thus can intercept any information passed through it. At the same time, an adversary can always perform certain form of DOS attack (e.g., jamming) even if it does not have any knowledge of the crypto-system used in the WSN.

One remedial solution to these attacks is to exploit the network's routing functionality. Specifically, if the locations of the black holes formed by the compromised (or jammed) nodes are known a priori, then information can be delivered over paths that circumvent (bypass) these holes, whenever possible. In practice, due to the difficulty of acquiring such location information, the above idea is implemented in a probabilistic manner, typically through a two-step process: secret sharing and multi-path routing.

We argue that three security problems exist in the counter-attack approach. First, this approach is no longer valid if the adversary can selectively compromise or jam nodes. This is because the route computation in the above multi-path routing algorithms is deterministic in the sense that for a fixed topology, a fixed set of routes is always computed by the routing algorithm for given source and destination. Therefore, even if the shares can be distributed over different routes, overall they are always delivered over the same set of routes that are computable by the algorithm. As a result, once the routing algorithm becomes open to the adversary (this can be done, e.g., through a memory interrogation of the compromised nodes), the adversary can by itself compute the set of routes for any given source and destination. Then the adversary can pinpoint to one particular node in each route and compromise (or jam) these nodes. Such an attack can intercept all shares of the information, rendering the above counter-attack approaches ineffective. Second, as pointed out in, actually very few node-disjoint routes can be found when node density is moderate and source and destination nodes are several hops apart. For example, for a node degree of 8, on average only two node-disjoint routes can be found between a source and a destination that are at least 7 hops apart. There is also a 30% possibility that no node-disjoint paths can be found between the source and the destination. The lack of enough routes significantly undermines the security performance of this multi-path approach. Last, even worse, because the set of routes is computed under certain constraints, the routes may not be spatially dispersive enough to circumvent a moderate-sized black hole.

In this paper, we present an efficient key management scheme and a randomized multipath routing algorithm that only needs small storage space less energy consumption. Contribution of this paper is of three folds. First, we utilize the C-neighbor concept and a key management scheme for power full sensors. Second, establishing keys among sensors using ECC public key cryptosystem. Third, developing distributed multipath routing algorithms based on the information available to the sensors. The schemes proposed are Non-Repetitive random propagation (NRRP) and Multi cat tree assisted random propagation (MTRP). The rest of the paper is organized as follows. Section II describes the proposed key management scheme. Section III describes the proposed multi path routing algorithm. Section IV describes the simulation results of the proposed schemes. Section V describes the conclusion.

2. PROPOSED KEY MANAGEMENT SCHEME

2.1 The Cluster Formation

After sensor deployment, clusters are formed in an HSN. We have designed an efficient clustering scheme for HSNs in. Because of the page limit, we will not describe the details of the clustering scheme

International Journal of Innovations & Advancement in Computer Science
IJIACS
ISSN 2347 – 8616
Volume 6, Issue 9
September 2017

here. For the simplicity of discussion, assume that each H-sensor can communicate directly with its neighbour H-sensors (if not, then relay via L-sensors can be used). All H-sensors form a backbone in an HSN. After cluster formation, an HSN is divided into multiple clusters, where H-sensors serve as the cluster heads. An illustration of the cluster formation is shown in Figure 1, where the small squares are L-sensors, large rectangular nodes are H-sensors, and the large square at the bottom-left corner is the sink.

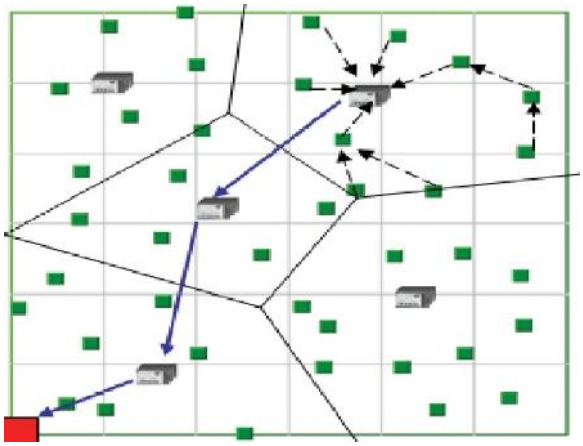

Figure 1. Cluster Formation in HSN

2.2 Distributed Key Establishment

The key setup can also be done in a distributed way. In the distributed key establishment, each L-sensor is pre-loaded with a pair of ECC keys - a private key and a public key. When an L-sensor (denoted as u) sends its locations information to its cluster head H, u computes a Message Authentication Code (MAC) over the message by using u's private key, and the MAC is appended to message. When H receives the message, H can verify the MAC and then authenticate u's identify, by using u's public key. Then H generates a certificate (denoted as CAu) for u's public key by using H's private key.

After determining the routing tree structure in a cluster, the cluster head H disseminates the tree structure (i.e., parent-child relationship) and the corresponding public key certificate to each L-sensor. The public key certificates are signed by H's private key, and can be verified by every

L-sensor, since each L-sensor is preloaded with H's public key. A public key certificate proves the authenticity of a public key and further proves the identity of one L-sensor to another L-sensor.

If two L-sensors are parent and child in the routing tree, then they are c-neighbours of each other, and they will set up a shared key by themselves. For each pair of c-neighbours, the sensor with smaller node ID initiates the key establishment process. For example, suppose that L-sensor u and v are c-neighbors and u has a smaller ID than v. The process is presented below:

1) Node u sends its public key KuU = IuP to v.

2) Node v sends its public key KvU = IvP to u.

3) Node u generates the shared key by multiplying its

private key Iu with v's public key - KvU , i.e., Ku,v = KuRKvU = IuIvP ; similarly, v generates the shared key = KvRKuU = IuIvP .

After the above process, nodes u and v share a common key and they can start secure communications. To reduce the computation overhead, symmetric encryption algorithms are used among L-sensors. Note that in the distributed key establishment scheme, the assumption of having tamper-resistant hardware in H-sensors can be removed.

3. PROPOSED RANDOMIZED MULTIPATH ALGORITHM

3.1. Overview

As illustrated in Figure 2, we consider a 3-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, e.g., the Shamir's algorithm. Each share is then transmitted to some randomly picked neighbor. That neighbor will continue to relay the share it has received to other randomly picked neighbors, and so on. In each information share, there is a TTL field, whose initial value is set by the source node to control the total number of randomized relays. After each relay, the TTL field is reduced by 1. When the TTL count reaches 0, the final node receiving this share stops the random propagation phase and begins to route this share towards the sink using normal single-path routing. Once the sink collects at least T shares, it can inversely compute the original

International Journal of Innovations & Advancement in Computer Science
IJIACS
ISSN 2347 – 8616
Volume 6, Issue 9
September 2017

information. No information can be recovered from less than T shares.

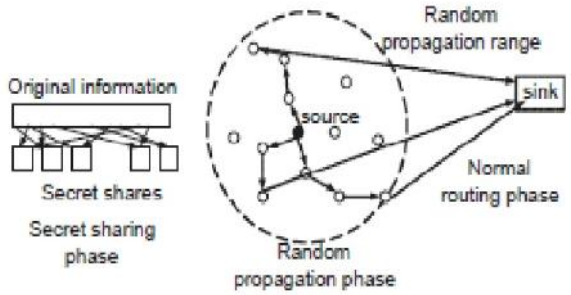

Figure 2. Randomized Dispersive routes

Because routes are randomly generated, there is no guarantee that different routes are still node-disjoint. However, the algorithm should ensure that the randomly generated routes are as dispersive as possible, i.e., different routes are geographically separated as far as possible such that they have high likelihood of not simultaneously passing through a black hole. Considering the stringent requirement on energy consumptions in WSNs, the major challenge in our design is to generate highly dispersive random routes at low energy cost.As explained later, such a challenge is not trivial. A naive algorithm of generating random routes, such as Wanderer scheme (a pure random-walk algorithm), only leads to long paths (containing many hops, and therefore, consuming much energy) without achieving good dispersiveness. Due to security considerations, we also require that the route computation be implemented in a distributed way, such that the final route represents the aggregate decision of all the nodes participating in route selection. As a result, a small number of colluding/compromised nodes cannot dominate the selection result. In addition, for efficiency purposes, we also require that the randomized route selection algorithm only incurs a small amount of communication overhead. Needless to say, the random propagation phase is the key component that dictates the security and energy performance of the entire mechanism.

3.2. Random propagation of Information Shares

To diversify routes, an ideal random propagation algorithm propagates information shares as dispersive as possible. Typically, this means propagating the share farther from its source. At the same time, it is highly desirable to have an energy-efficient propagation, which calls for limiting the number of randomly propagated hops. The challenge here lies in the random and distributed nature of the propagation: a share may be sent one-hop farther from its source in a given step, but may be sent back closer to the source in the next step, wasting both steps from the security's point of view. To tackle this issue, some control needs to be imposed on the random propagation process to ensure that in each step the share is more likely to be forwarded outwards from the source. We develop four distributed random propagation mechanisms, which approach this goal in various degrees.

Non-repetitive Random Propagation: NRRP is based on PRP, but it improves the propagation efficiency by recording all the nodes that the propagation has traversed so far. More 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 up-stream node is appended to the share's NIR field. Nodes included in NIR are excluded from the random pick of the next hop of propagation. 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.

Multicast Tree-assisted Random Propagation: The MTRP scheme aims at actively improving the energy efficiency of random propagation while preserving the dispersiveness of DRP. The basic idea comes from the following observation of Figure 2: Among the 3 different routes taken by the shares, the route on the bottom right is the most energy efficient because it has the shortest end-to-end path. So, in order to improve energy efficiency, the 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 Figure 2.

MTRP involves directionality in its propagation process without needing location information. More specifically, after the deployment of the WSN, MTRP requires that the sink constructs a multicast tree from itself to every node in the network. Such a tree-construction operation is not unusual in existing protocols, and is typically conducted via flooding a "hello" message from the sink to every node. Once this multicast tree is constructed, a node knows its distance (in number of hops) to the sink and the id of its parent node. We assume that each entry in the neighbor list maintained by a node has a field recording the number of hops to the sink from the corresponding neighbor. Under MTRP, the header of

each share contains two additional fields: maxhop and minhop. The values of these two parameters are set by the source to maxhop = ns + α1 and minhop = ns - α2, where ns is the hop count from the source to the sink, and α1 and α2 are nonnegative integers with α1 ≤ α2. The parameter α1 controls the limit that a share can be propagated away from the sink, i.e., to the left half of the circle in Figure 1. The parameter α2 controls the propagation area toward the sink, i.e., the right half of the circle. A small α2 makes the propagation of a share be dispersed away from the centre line connecting the source and the link and forces them to take the side path, leading to better dispersion.

Before a node begins to pick the next relaying node from its neighbor list, it first filters out neighbors that are in the LHNL, just as in the case of DRP. Next, it filters out nodes that have a hop count to the sink greater than maxhop or smaller than minhop. The next relaying node will be randomly drawn from the remaining neighbors. In case the set of remaining nodes after the first step is empty, the second step will be directly applied to the entire set of neighbors.

5. CONCLUSION

The proposed key management scheme utilizes the fact that a sensor only communicates with a small portion of its neighbors and thus greatly reduces the communication and computation overheads of key setup. A public key algorithm – Elliptic Curve Cryptography (ECC) is used to further improve the key management scheme. The scheme only pre-loads a few keys on each L-sensor and thus significantly reduces sensor storage requirement. Our performance evaluation and security analysis showed that the routing-driven, ECC-based key management scheme can significantly reduce communication overhead, sensor storage requirement and energy consumption while achieving better security than a popular key management scheme for sensor networks.

6.REFERENCES

[1]Gupta and P. R. Kumar, “The capacity of wireless networks,” IEEE Trans. Inform. Theory, vol IT-46, no. 2, pp. 388-404, Mar. 2000.

[2]E. J. Duarte-Melo and M. Liu, “Data-gathering wireless sensor net-works: organization and capacity,” Computer Networks (COMNET) Special Issue on Wireless Sensor Networks, vol. 43, no. 4, pp. 519-537, Nov. 2003.

[3]K. Xu, X. Hong, and M. Gerla, “An ad hoc network with mobile backbones,” in Proc. IEEE ICC 2002, New York, NY, Apr. 2002.

[4]L. Girod, T. Stathopoulos, N. Ramanathan, et al., “A system for simu-lation, emulation, and deployment of heterogeneous sensor networks,” in Proc. ACM SenSys 2004.

[5]M. Yarvis, N. Kushalnagar, H. Singh, et al., “Exploiting heterogeneity in sensor networks,” in Proc. IEEE INFOCOM 2005, Miami, FL, Mar. 2005.

[6]L. Eschenauer and V. D. Gligor, “A key management scheme for distributed sensor networks,” in Proc. 9th ACM Conference on Com-puterand Communication Security, pp. 41-47, Nov. 2002.

[7]H. Chan, A. Perrig, and D. Song, “Random key predistribution schemes for sensor networks,” in Proc. 2003 IEEE Symposium on Security and Privacy, May 2003, pp. 197-213.

[8]K. Whitehouse, C. Sharp, E. Brewer, and D.Culler, “Hood: a neighborhood abstraction for sensor networks,” in Proc. ACM International Conference on Mobile Systems, Applications,and Services (MobiSys ’04), Boston, MA, June, 2004.

[9]R. Cristescu and B. Beferull-Lozano, “Lossy network correlated data gathering with high-resolution coding,” in Proc. IEEE IPSN 2005.

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

AUTHOR’S INFORMATION

1N.Sainath B.Tech CSE from Jaya Prakash Narayana College of Engineering, M.Tech SE from Srinidhi Institute of Technology. Currently he is working as Associate Professor at St.Martins Engineering College. His areas of interest include Data mining, Network Security, Software Engineering, Sensor Networks, and Cloud Computing. He is enrolled for the Professional

memberships of IEEE, CSI, MISTE, IAENG, CSTA. He has Published 22 papers in International Journals and has 12 International conference Proceedings and attended 12 workshops and 10 National conferences.

2.M.Ravi Kumar, M.Tech from Dr.M.G.R.Education & Research Institute, Chennai in 2005. Currently working as Professor for the department of CSE in JBREC Hyderabad and he is a Research Scholar of KL University, Vijayawada. His areas of interest include Cloud Computing, Network Security, Data Mining, Software Engineering. He has Published 2 papers in International Journals and has 1 International conferenceProceedings.

3.Dr.U.Moulali PhD from Annamalai University .Currently working as Professor for the department of CSE in JBREC Hyderabad . He has a vast teaching experience and Published many research papers in various Reputed Journals & has attended Several International Conferences. He is Enrolled for the memberships of CSI & ISTE. His areas of interest are Data mining , Network Security , Artificial Intelligence, Ad-hoc Networks.

4.A.Prakash Currently working as Head of the Department in St Martins Engineering College.He Completed his M.tech in Software Engineering from JNTUH.He has an experience of 12 years in teaching and his areas of interest are Education Techbnologies , Computer Networks , Cryptography & Security