EXCELLENT PUBLISHERS

International Journal of Current Research and Academic Review

ISSN: 2347-3215 Volume 2 Number 8 (August-2014) pp. 345-355

www.ijcrar.com

On the Node Clone Detection in Sensor Networks for Electronic Copy Right Management System

K.B.Gopi Krishnan[1] **and K.R.Ananthapadmanaban**[2*]

[1]Department of I.T Saveetha school of Engineering, Saveetha University, Chennai, India
[2]Department of Computer Science, SRM Arts & Science Colledge, Kattankulathur, Tamilnadu, India
****Corresponding author***

KEYWORDS

Destination zone, travel node, primary node, secondary node, tertiary node

ABSTRACT

Wireless sensor networks are susceptible to node clone. So several distributed protocols have been proposed to detect this attack. On the other hand, they require too strong assumptions to be practical for large-scale at random deployed sensor networks. In this research paper, we propose two novel node clone detection protocols with different tradeoffs on network conditions and performance. The initial one is based on a distributed hash table (DHT) by a fully decentralized key-based caching and checking system which is constructed to catch cloned nodes effectively. The protocol performance on efficient storage space consumption and towering security level is theoretically deducted through a probability representation and the resulting equations with necessary adjustments for real application which are supported by simulations. The next distributed detection protocol named randomly directed exploration. The simulation results uphold the protocol design and explain its efficiency on communication overhead and satisfactory result probability. Electronic copyright management systems (ECMS) automatically manage the issues related to trading multimedia documents through open communication networks. Integration of cryptography with watermarking technologies can provide intellectual property rights (IPR) protection in an open network environment such as the Internet.

Introduction

The main aim of the research is the progress of efficient wireless sensor networks with high security point and holds strong resistance against adversary's assault. It is projected to provide highly efficient communication presentation with adequate detection probability for bulky sensor networks. With many physical attacks to sensor networks, the node clone is a serious and dangerous one to Production expense limitation, sensor nodes are generally short of tamper-resistance hardware components. Thus, an adversary can capture a few nodes, extract code and all secret testimonials and use that equipment to clone many nodes out of off-the-shelf sensor hardware. Those cloned nodes seem that legitimate can freely join the sensor network and then significantly enlarge the adversary's capacities to direct the network maliciously.

Wireless Sensor Network (WSN) with spatially distributed autonomous are used to monitor physical or environmental conditions such as temperature, sound, pressure, etc.. The modernized Wireless Sensor Networks are bi-directional enabling the control of sensor activity. The Wireless Sensor Networks are developed such that they are useful in military applications as battlefield surveillance. Now a day's these networks are also used in many industrial consumer applications like industrial process monitoring, health monitoring etc.

Sensor nodes are small computers usually consisting of a processing unit with an average computational power, limited memory, sensors or MEMS, a communication device (usually radio transceivers or alternatively optical) and a power source usually in the form of a battery.

Need of this Research

The low-cost of off-the-shelf hardware components in unshielded sensor-network nodes leave them vulnerable to compromise. With a little effort, the adversary can capture nodes, analyse and replicate them and surreptitiously insert these replicas at strategic locations within the network. These attacks have severe consequences and allow the adversary to corrupt network data or even disconnect significant parts of the network. Previous node replication detection schemes depend primarily on centralized mechanisms with single points of failure, or on neighbourhood voting protocols that fail to detect distributed replications. To address these fundamental limitations, we propose two new algorithms based on emergent properties. The first property is that arise only through the collective action of multiple nodes. The second property is Randomized multicast distributed node location information to randomly-selected witnesses, exploiting the birthday paradox to detect replicated nodes while line-selected multicast uses the topology of the network to detect replication. Both of the algorithms provide globally-aware, distributed node-replica detection and line-selected multicast displays particularly strong performance characteristics. We show that emergent algorithms also represent a promising new approach to sensor network security. Moreover, the results naturally extend to other classes of networks in which nodes can be captured, replicated and re-inserted by an adversary.

Overall System Design Structure

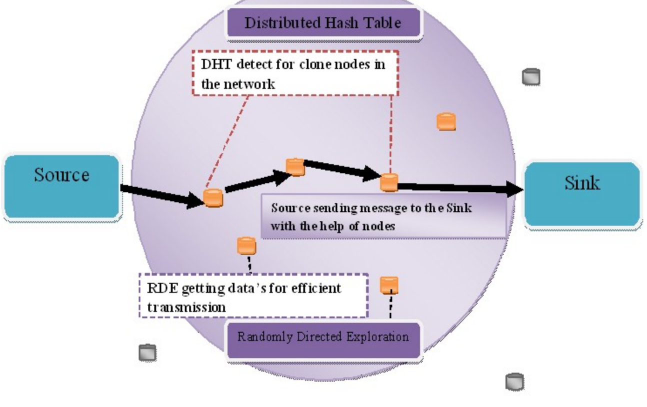

Distributed Hash Table
DHT detect for clone nodes in the network
Source
Sink
Source sending message to the Sink with the help of nodes
RDE getting data's for efficient transmission
Randomly Directed Exploration

Fig.1 Overall System Design Structure

Module Description

There are six modules which are used in this research and they are listed below:

- Setting up Network Model
- Initialization Process
- Claiming Neighbour's Information
- Processing Claiming Message
- Sink Module
- Performance Analysis

Setting up Network Model

The first module is "setting up the network model". On considering a large-scale homogeneous sensor network having resource-constrained sensor nodes. Analogous to previous distributed detection approaches we assume that an identity-based public-key cryptography facility is available in the sensor network. Prior to deployment, each legitimate node is allocated a unique ID and a corresponding private key by a trusted third party. The public key of a node is its ID which is the essence of an identity-based cryptosystem. Consequently, no node can lie to others about its identity. Moreover, anyone is able to verify messages signed by a node using the identity-based key. The source nodes in the problem formulation serve as storage points which cache the data gathered by other nodes and periodically transmit to the sink in response to user queries. Such network architecture is consistent with the design of storage centric sensor networks

Initialization Process

To activate all nodes for starting a new round of node clone detection, the initiator uses a broadcast authentication scheme to release an action message including a monotonously increasing nonce, a random round seed, and an action time. The nonce is intended to prevent adversaries from launching a DOS attack by repeating broadcasting action messages.

Claiming Neighbour's Information

Receiving upon an action message, a node verifies "if the message nonce is greater than the last nonce and if the message signature is valid". If both pass, the node updates the nonce and stores the seed. The node operates as an observer that generates a claiming message for each neighbour (examinee) and transmits the message through the overlay network with respect to the claiming probability at the designated action time. Nodes start transmitting claiming messages. The huge traffic can cause serious interference and degrade the network capacity at the same time. To relieve this problem, we may specify a sending period during the nodes randomly for picking up a transmission time for every claiming message.

Processing Claiming Messages

Claiming message shall be forwarded to its destination node via several Chord intermediate nodes. Only those nodes in the overlay network layer (i.e., the source node, Chord intermediate nodes, and the destination node) need to process a message whereas the other nodes along the path simply route the message to temporary targets. Algorithm 1 for handling a message is the kernel of our DHT-based detection protocol. If the algorithm returns NIL, the message has arrived at its destination. Otherwise, the message can be subsequently forwarded to the next node with the ID that is returned.

Sink Module

Sink is the point of contact for users of the sensor network. Every time the sink receives a question from a user. First of all it translates the question into multiple queries and disseminates the queries to the corresponding mobile relay which process the queries based on their data and return the query results to the sink. The sink unifies the query results arising from multiple storage nodes to the final answer and sends it back to the user.

Performance Analysis

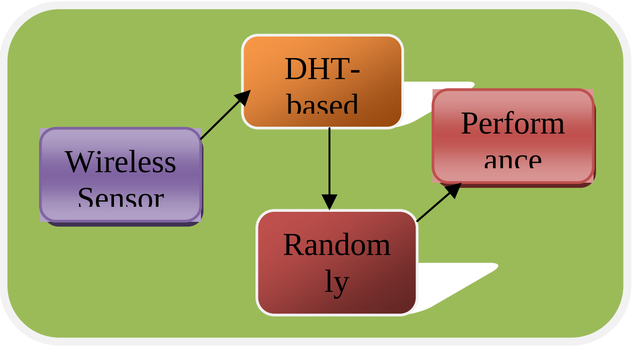
For the Distributed Hash Table (DHT) based detection protocol, we use the following specific measurements to evaluate its performance.

(i) Average number of transmitted messages which represents the protocol's communication cost.

(ii) Average size of node cache tables stands for the protocol's storage consumption.

(iii) Average number of witnesses serves as the protocol's security level because the detection protocol is deterministic and symmetric.

Control Flow Diagram



System Implementation

Motivation and Problem Statement

Generally, wireless sensor networks consist of hundreds and thousands of low cost, resource-constrained, distributed sensor nodes which usually scatter in the surveillance area randomly working without attendance. If the operation environment is hostile, security mechanisms against adversaries has to be taken into consideration. For example, those vicious nodes occupy strategic positions and cooperatively corrupt the collected information. The adversary may even gain control of the whole network with a large number of cloned nodes under command. Furthermore, the node clone can exacerbate most of the inside attacks against sensor networks. So we present two novel that practical node clone detection protocols with different trade-offs on network conditions and performance.

Description of Research

Generally, countermeasures against node clone can be categorized into three categories: prevention schemes that inherently forbid cloned nodes to join network, centralized detection in which there exists a central powerful party responsible for receiving reports and making judgements of node clone, distributed detection where all nodes cooperatively process information and detect node clone in a distributed

Techniques and Protocol Used

1. Distributed Hash Table (DHT)
2. Randomly Directed Exploration

Distributed Hash Table (DHT)

Distributed Hash Table (DHT) which a fully decentralized, key-based caching and checking system is constructed to catch cloned nodes. The protocol's performance on memory consumption and critical security metric are theoretically deducted through a probability model and the resulting equations with necessary adjustment for real application which are supported by simulations. Our analysis shows the comprehensive simulation results that the DHT-based protocol can detect node clone with high security level and holds strong resistance against adversary's attacks.

The principle of our first distributed detection protocol is to make use of the DHT mechanism to form a decentralized caching and checking system that can effectively detect cloned nodes. Essentially, DHT enables sensor nodes to distributive construct an overlay network upon a physical sensor network and provides an efficient key-based routing within the overlay network. A message associated with a key can be transmitted through the overlay network to reach a destination node that is solely determined by the key; the source node does not need to specify or know which node a message’s destination is the DHT key-based routing takes care of transportation details by the message’s key. More importantly, messages with a same key will be stored in one destination node. Those facts build the foundation for our first detection protocol. As the beginning of a round of DHT-based clone detection, the initiator broadcasts the action message including a random seed.

Every observer constructs a claiming message for each neighbour node, which is referred to as an examinee of the observer and the message, and sends the message with probability P_c independently. The introduction of the claiming probability P_c is intended to reduce the communication overwork in case of a high-node-degree network. In the protocol, a message’s DHT key that determines it’s routing and destination is the hash value of concatenation of the seed and the examinee’s ID. By means of the DHT mechanism, a claiming message can eventually be transmitted to a deterministic destination node which can cache the ID-location pair and check for node clone detection, actingas an inspector. In addition, some intermediate nodes also behaves inspectors to improve resilience against the adversary in an efficient way.

Before diving into the detection protocol, we briefly introduce DHT techniques. In principle, a distributed hash table is a decentralized distributed system that provides a key-based lookup service similar to a hash table: (key, record) pairs are stored in the DHT and any participating node can efficiently store and retrieve records associated with specific keys. By design, DHT distributes responsibility of maintaining the mapping from keys to records among nodes in an efficient and balanced way which allows DHT to scale to extremely large networks and be suitable to serve as a facility of distributed node clone detection.

There are several different types of DHT proposals such as CAN Chord and Pastry. Generally, CAN hasleast efficiency than others in terms of communication cost and scalability, and it is rarely employed in real systems. By contrast, Chord is widely used and we choose Chord as a DHT implementation to demonstrate our protocol. However, our protocol can easily migrate to build upon Pastry and present similar security and performance results. The technical core of Chord is to form a massive virtualring in which every node is located at one point owning a segment of the periphery. To achieve pseudo-randomness on output, a hash function H is used to map an arbitrary input into a-bit b space which can be conceived as a ring.

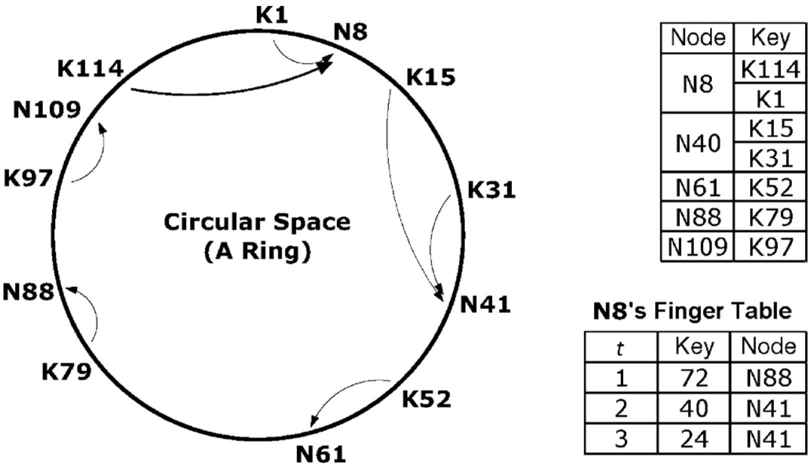
Each node is assigned with a Chord coordinate upon joining the network. Practically for our protocol, a node’s Chord point’s coordinate is the Fig 3 Chord network example where the key space is 7-bit; seven records with different keys are stored in five nodes and the successor table size. For node, its direct predecessor and its two successors are hash value of the node’s MAC address. All □ nodes divide the ring into □ segments by their Chord points. Likewise, the key of a record is the result of the hash function. Every node is responsible for one segment that ends at the node’s

Table.1 Comparison among the Distributed Detection Protocols

Protocols	Requirements for nodes	Communication Cost	Memory Cost	Detection Level
Randomized Multicast	Awareness of all nodes	O(n)	O(d√(n)	Acceptable
Line Selected Multicast	Awareness of all nodes	O(√n)	O√(n)	Acceptable
Proposed DHT based Protocol	DHT nodes information	O(log n√(n)	O(d)	Strong
Proposed randomly distributed exploration	Neighbours information	O(√(n)	O(d)	Good

Table.2 Four Roles in the Proposed Detection Protocols

Roles	**Trusted**	**Duty**
Initiator	Yes	Start a round of detection
Observer	No	Claims neighbour IDs and locations
Inspector	No	Buffer and check messages for detection
Witness	No	Broadcast detection evidence



Node	Key
N8	K114 K1
N40	K15 K31
N61	K52
N88	K79
N109	K97

N8's Finger Table

t	Key	Node
1	72	N88
2	40	N41
3	24	N41

Fig.3 Chord Network Example

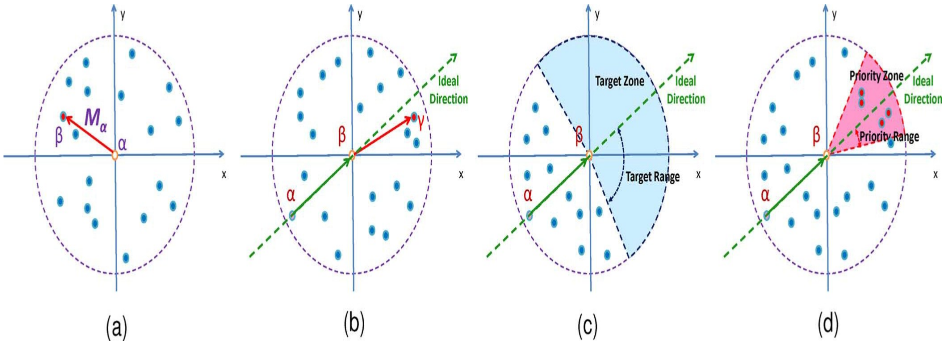


Fig.4 Routing mechanisms in the randomly directed exploration protocol. (a) Initial random direction. (b) Deterministic directed. (c) Border determination.(d) Probabilistic directed.

Chord point, and all records whose keys fall into that segment will be transmitted to and stored in that node. As the kernel of efficient key-based routing, every node maintains, a finger table of size t=O (log n) to facilitate a binary-tree search. Specifically, the finger table for a node with Chord coordinate **y** contains information of nodes that are respectively responsible for holding the keys: $(y+^{2b-i})$ mod 2^b for i € [1, t]. If two nodes are within g the ring segments distance, they are each other's predecessor and successor by the order of their coordinates with respect to predefined 'g'. In theory, a Chord node only needs to know its direct predecessor and finger table. To improve resilience against network churn and enhance routing efficiency, every node additionally maintains a successor table containing its successors.

Typical values of gare between 10 and 20. A demonstrative example of a Chord system with small parameters is given in Fig 3 In this system, if node N8 wants to query a record with K97key,it first looks up its successor table. Since 97 is not in (109, 61), namely (direct predecessor, the last successor), node N8 proceeds with the finger table and finds that the next forwarding node N88 should be because 97€ (72): the first item in finger table corresponding to, 109: direct predecessor. When receives this query about, by checking its successor table with two nodes of and it determines the destination should be, as N88: itself, 109: the first successor. By this routing mechanism, on average $g \div (g+1)$of queries toward a destination pass through one of g predecessors. For node N109 as the destination, its two predecessors are N88 and N61 and the latter's direct predecessor is N41. The line from N109 and N41 has the length of 109-41=68 and is divided by N61 and N88 into three segments with lengths of 61-41=20, 88-61=27 and 109-88=21. Therefore, the probabilities of a query passing through N61 and N88 are 20/68 and 27/68.

Protocol Details

As a prerequisite, all nodes cooperatively build a Chord overlay network over the sensor network. Cloned node may not participate in this procedure but it does not give themany advantage of avoiding detection. The construction of the overlay network is independent of node clone detection. As a result, nodes possess the information of their direct predecessor and successor in the Chord ring. In addition, each node caches information of its g consecutive successors in its successorstable. Many Chord systems utilize this kind of cache mechanism to reduce the communication cost and enhance systems robustness. More importantly in our protocol, the facility of the successors table contributes to the economical selection of inspectors.

Randomly Directed Exploration

The DHT-based detection protocol can be applied to general sensor networks, and its security level is remarkable as cloned nodes can be caught by one deterministic witness plus several probabilistic witnesses. However, the message transmission over a Chord overlap network incurs considerable communication cost which may not be desired for some sensor networks that are extremely sensitive to energy consumption. To fulfil this challenge, we propose the randomly directed exploration (RDE) which tremendously reduces communication cost and presents optimal storage expense with adequate detection probability.

The RDE protocol shares the major merit with broadcasting detection: every node only needs to know and buffer a neighbour-list containing all neighbours IDs and locations. For both detection procedures, every node constructs a claiming message with signed version of its neighbour-list and then tries to deliver the message to others which can compare with its own neighbour-list to detect clone. For a dense network, broadcasting will drive all neighbours of cloned nodes to find the attack but in fact one witness that successfully catches the clone and then notifies the entire network could suffice for the detection purpose.

To achieve that in a communicatively efficient way, we bring several mechanisms and effectively construct a multicast routing protocol. First, a claiming message needs to provide maximal hop limit and initially it is sent to a random neighbour. The message subsequent transmission can roughly maintain a line. The line transmission property helps a message to go through the network as fast as possible from a locally optimal perspective. In addition, we introduce border determination mechanism to significantly reduce communication cost.

We can do all of those because every node is aware of its neighbours locations which is a basic assumption for all witness-based detection protocols but rarely utilized by other protocols.

Protocol Description

One round of clone detection is still activated by the initiator. Subsequently, it creates its own neighbour-list including the neighbour's IDs and locations which constitutes the sole storage consumption of the protocol. As an observer for all its neighbours, it starts to generate a claiming message containing its own ID, location, and its neighbour-list.

There are three main mechanisms used in this process and they listed below

Deterministic Directed Transmission

When node receives a claiming message from previous node, the ideal direction can be calculated. In order to achieve the best effect of line transmission, the next destination node should be node which is closest to the ideal direction.

Network Border Determination

It takes network shape into consideration to reduce the communication cost. In many sensor network applications, there exist outside borders of network due to physical constrains. When reaching some border in the network, the claiming message can be directly discarded. In our proposal for border local determination, another parameter target range is used along with ideal direction to determine a target zone. When no neighbour is found in this zone, the current node can conclude that the message has reached a border and throw it away.

Probabilistic Directed Transmission

In the probabilistic directed transmission, parameter priority range along with the ideal direction is used to specify a priority zone, in which the next node can be selected. When no nodes are located in that zone, the deterministic directed candidate within the target zone can be selected as the next node. If there are several nodes in the priority zone, their selection probabilities are proportional to their angle distances to priority zone border. In this way, the desired line transmission property is reserved, while a certain extent of important randomness is introduced.

This is intended to provide high efficient communication performance and adequate detection probability for denser sensor networks. In the protocol, initially nodes send claiming messages containing a neighbour-list along with a maximum hop limit to randomly selected neighbours, the subsequent message transmission is regulated by a probabilistic directed technique to approximately maintain a line property through the network as well as to incur sufficient randomness for better performance on communication and resilience against adversary.

In addition, border determination mechanism is employed to reduce communication payload. During forwarding, intermediate nodes explore claiming messages for node clone detection. By this design, the protocol consumes almost minimal memory and the simulations show that it out performs all other detection protocols in terms of communication cost, while the detection probability is satisfactory. In the above section, we analyze certain important aspects under ECMS. By digital water marking technique, we send secret data among four prominent players. They are Author module, Collection society module, Buyer module, Control authority module.

System Study

The feasibility of the research is analysed in this phase and business proposal is put forth with a very general plan for the research and some cost estimates. During system analysis, the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, it is necessary to understand some of the major requirements of the system. Three key considerations involved in the feasibility analysis are:

(i) ECONOMICAL FEASIBILITY
(ii) TECHNICAL FEASIBILITY
(iii) SOCIAL FEASIBILITY

System Testing

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub-assemblies, assemblies and a finished product. It is the process of exercising software with the intent of ensuring that the software system meets its requirements and user expectation. There are various types of test. Each test type addresses a specific testing requirement.

Conclusion

Sensor nodes lack tamper-resistant hardware is subject to the node clone attack. In this research paper, we propose two distributed detection protocols. First one is based on a distributed hash table which forms a Chord overlay network and provides the key-based routing caching and checking facilities for clone detection. Second one uses probabilistic directed technique to achieve efficient communication overhead for satisfactory detection probability. While the DHT-based protocol provides high security level for all kinds of sensor networks by one deterministic witness and additional memory-efficient, probabilistic witnesses.

DHT-based protocol can effectively detect clone for general sensor networks with high security level and efficient storage consumption, while its communication cost is in the same order of magnitude with previous detection schemes sensor networks e.g., virtual cord protocol. As more and more low-bit rate compression standards for video are emerging and with the progress of wireless technology, a lot of challenges are now thrown to video watermarking a simple extension of image watermarking method could not be enough.

The Randomly Directed Exploration presents outstanding communication performance with minimal storage consumption for denser sensor networks. From exploration protocol outperforms all other distributed detection protocols in terms of communication cost and storage requirements, while its detection probability is satisfactory, higherthan that of line-selected multicast scheme. In addition, all nodes only need to know their direct neighbour's information and inherent routing technique delivers messages in an efficient way to cover great range of the network.

Scope for Further Development

In the future work, we would like to explore additional mechanisms to ensure that the protocols continue to function even in the face of misbehaving nodes. For example, McCune et al. describe a technique that uses secure implicit sampling to detect nodes that suppress or drop messages. We could also use some of the techniques like High Noon and Time Slots to periodically sweep the network for replicas, thus preventing the adversary from establishing a significant foothold in the network. Line-Selected Multicast provides excellent resiliency while achieving near optimal communication overhead with only modest memory requirements.

This research is tested with sample data and found to be executing at its maximum performance. This research has been developed to satisfy the users to send messages in more secure and efficient manner. This proposed scheme may be further enhanced and used in copyright protection. In addition, the entire image format should be supported by software. The e-commerce to be, used in e-transaction can be added in future.

References

Parno, B., A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in Proc. IEEE Symp. Security Privacy, 2005, pp. 49–63.

Balakrishnan, H., M. F. Kaashoek, D. Karger, R. Morris, and I. Stoica, "Looking up data in P2P systems," Commun.ACM, vol. 46, no. 2, 2003.pp. 43–48

Zhang, Y.,W. Liu,W. Lou, andY. Fang, "Location-based compromise tolerant security mechanisms for wireless sensor networks," IEEE J. Sel. Areas Commun., vol. 24, no. 2, Feb. 2006,pp. 247–260.

Zhu, S., S. Setia, and S. Jajodia, "LEAP: Efficient security mechanisms for large-scale distributed sensor networks," in Proc. 10th ACM CCS, Washington, DC, 2003, pp. 62–72.

Anderson, R., H. Chan, and A. Perrig, "Key infection: Smart trust for smart dust," in Proc. 12th IEEE ICNP, 2004, pp. 206–215.

Conti, M., R. D. Pietro, L. V. Mancini, and A. Mei, "A randomized, efficient, and distributed protocol for the detection of node replication attacks inwireless sensor networks," in Proc. 8thACMMobiHoc,Montreal, QC, Canada, 2007, pp. 80–89.

Zhu, B., V. G. K. Addada, S. Setia, S. Jajodia, and S. Roy, "Efficient distributed detection of node replication attacks in sensor networks," in Proc. 23rd ACSAC, 2007, pp. 257–267.

Choi, H., S. Zhu, and T. F. La Porta, "SET: Detecting node clones in sensor networks," in Proc. 3rd SecureComm, 2007, pp. 341–350.

Brooks, R., P. Y. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M. T. Kandemir, "On the detection of clones in sensor networks using random key predistribution," IEEE Trans. Syst.s, Man, Cybern. C, Appl. Rev., vol. 37, no. 6, Nov. 2007, pp. 1246–1258.

Eschenauer, L. and V. D. Gligor, "A key-management scheme for distributed sensor networks," in Proc. 9th ACM Conf. Comput.Commun. Security, Washington, DC, 2002, pp. 41–47.

Shamir, A., "Identity-based cryptosystems and signature schemes," in Proc. CRYPTO, 1984, LNCS 196, pp. 47–53.

Poovendran, R., C. Wang, and S. Roy, Secure Localization and Time Synchronization for Wireless Sensor and Ad Hoc Networks. New York: Springer-Verlag, 2007.

Akyildiz, I. F., W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Commun. Mag., vol. 40, no. 8, Aug. 2002., pp. 102–114.

Ratnasamy, S., P. Francis, M. Handley, R. Karp, and S. Schenker, "A scalable content-addressable network," in Proc. SIGCOMM, San Diego, CA, 2001, pp. 161–172.

Stoica, I., R.Morris, D. Liben-Nowell, D. R. Karger,M. F.Kaashoek, F. Dabek, and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup protocol for internet applications," IEEE/ACM Trans. Netw., vol. 11, no. 1Feb. 2003, pp. 17–32.

Rowstron, A. I. T., and P. Druschel, "Pastry: Scalable, decentralized object location, and routing for large-scale peer-to-peer systems," in Proc. IFIP/ACM Int. Conf. Distrib. Syst. Platforms Heidelberg, 2001, pp. 329–350.