ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Detection of Replicas for Wireless Sensor Network Based On Low- Price and Energy Efficiency

Chavan Laxman, Prof. Bere S. S.

PG Scholar, Dept. of Information Technology, DGOIFOE, Bhigwan, Pune, India

Dept. of computer Engineering, DGOIFOE, Bhigwan, Pune, India

ABSTRACT: The wireless sensor nodes having the very great important in most of the sectors which are surrounded with the daily lives of users. Simultaneously it increases the new challenges in the Wireless Sensor Network's (WSN) security and also the end-user privacy. The one of most challenging problem in wireless sensor network is the detection of replicas attack. In the WSN once the sensor node actually captured then it is very easy to reprogramming it and then makes the large number duplicate copies of node i.e. replica, which may be misbehaves in the network. Hence for maintaining the network security and end user's privacy, it is necessary to detect it through the efficient way. There are lots of methods proposed for the detection of these replicas, but most of them require the costly hardware's like as the Global Positioning System (GPS). In general the prices of the sensor nodes are less as compared to GPS. This paper proposed a replicas detection scheme in static WSN with low price and energy-efficient way. For this proposed solution does not require any additional hardware such as GPS. Then also it gives the better result as compared to exiting system. Also the proposed system saves the lot of energy than exiting system.

KEYWORDS: Security and protection, authentication, network protocols, ubiquitous computing

I. INTRODUCTION

Now a day the wireless sensor networks are gaining the popularity in the no. of sectors. The WSN provides two different technologies such as: computation and communication which consists of large number of sensing devices and also support for physical and Environmental conditions like humidity, temperature, pressure, sound etc. In the WSN maintaining the security is quite difficult task, because the sensor nodes having the less hardware support. Data collected by the sensing devices is also transmitted to the destination known as the base station or sink. WSN's have various security challenges as compared to established network. The sensor nodes generally support for tamper resistances behind the hardware. In the WSN, once the attacker gains the credential of the sensor node then making the replicas is the very easy task for him/her. After that these created replicas are used to launching the different types of the attacks in WSN as per the attacker's intention. These attacks are called as the replicas attacks.

The demanding approaches i.e. the sensor node having the additional hardware is greatly increase the price of the conventional network. Accordingly, this paper introduces the low price replica detection system for static WSN by using "Bloom Filter" and "Sequential delivery algorithm" instead of using the external hardware like: GPS. The GPS is used in the conventional network to find out the physical location of the sensor node. But in the proposed approach each & every nodes having the unique id and the adjacent node ID's are used rather than the nodes location information to avoided the use on GPS. Neighboring nodes IDs also presented with constant size by using Bloom Filter. The "Bloom Filter Output"(BFO) is used as the proof. In the conventional method the traffic is gradually increased between the adjacent node and the randomly selected node. But in the projected scheme generate the weighty traffic by transmitting proofs form the starting. The scheme disperses the whole traffic on overall network and the whole result of this shows that the projected solution is more energy efficient than presented one.

DOI: 10.15680/IJIRCCE.2016. 0406364

The contribution of purposed solution as follows:

Low price: The projected scheme reduces the cost of structuring the large WSN for the replicas detection by avoiding the use of costly additional devices like as GPS. Instead of using the location information it uses the neighboring node ID's to identify the replica.

Energy competent discovery of replica: The projected scheme creates the less traffic rather than the conventional system. This is result in the less packet loss & faster transmission. Energy competence is very central in WSN. The node in surroundings are often non rechargeable and hence accessibility depends on energy efficiency.

Large scale network support: Due to the low price and the energy competent detection of the replica in WSN, the projected system is also supportive for the huge networks.

Replica Attack and Detection Scenario:

In the replica attack scenario, firstly the attacker obtains or makes the control over the sensor nodes which are deployed in the WSN. After that an attacker captures undisclosed information from them. Then, hacker or attacker creates the no. of copies of the original node using his secrete information and spread over the under attack area. Here, the adjacent nodes recognize replicas as newly deployed nodes. In the WSN the replica detection test is carried out for recognizing the duplicate nodes in the network. But the duplicate nodes i.e. replica also contain the secret information which obtained from the original nodes; because it is the copy of the original node. In the WSN each and every node must prove that it is legitimate node. Replicas should prove that they are nodes with valid secret information. On the other hand, replicas already know the secret information; they can easily provide the evidence that it is the neighboring nodes without any complexity. Hence, before proving the legitimacy, all newly inserted nodes (out of which some may be replicas) need to go through the replica detection test more than once.

While detection of the replicas, some assumptions are made. First one is, an attacker node does not generate a new ID for the created duplicate node. At that instance each and every node also having some secret keys which is already shared with his neighboring node and it is very difficult to track this key for the newly created replica. So, the replica does not get the more benefit by gaining the ID of the original node. Another assumption is, each and every node has one authentic adjacent node. One more assumption is that each and every node knows the ID's of nodes surrounded by two hops nodes; so every node can easily create the two hop node list and broadcast it with the encouragement packet. After receiving this packet the neighboring node arrange the reply packet and reply it. Then the sender node adds this node within his two hops nodes list. In this way every node create their own hop lists and finally exchange this list with each other to avoid the misleading of the replica.

Bloom Filter:

Commonly a Bloom filter is used for the member checking. A Bloom filter for representing a group G = {a1, a2…an} of n members is described by an array of m bits, initially all set to 0. A Bloom filter uses k independent one-way hash functions h1, h2 ….hk with range {1…m}. For mathematical expediency, make the natural assumption that these hash functions map each item in the universe to a random number uniform over the range {1 …m}. For each member a belongs to G and the bits between 1 to m are also set to 1. A location can be set to 1 multiple times, but only the first change has an effect. Hence, a Bloom filter suggests that a member a is in G even though it is not.

This section describes a projected replica detection method RDB-R. The main idea behind this method is to use adjacent node IDs of a newly created node and which may be a duplicate node or the replica. The neighboring node IDs are compacted and programmed by a Bloom filter successively. This encoded and the compressed set is used as evidence to detect replicas. Consequently, the validity of the proof is verified by comparing two Bloom filter outputs for the same node ID. We define the Bloom filter output comparison as the subset checking. The proposed solution basically contains the three stages; first one is the proof generation, second one is the proof validation and final one is the proof delivery.

II. RELATED WORK

The security and privacy are the major issues for internet of Things (IoT) applications; which is the main focus of the research in the previous decade and it still facing some massive challenges. In order to make easy this rising domain, need a detail review the research progress of IoT and make concentration on the security.

The replica discovery scheme used in presented system is vary very much according to their consumption strategies: *random consistent deployment* and *grid deployment.* In this the sensor nodes are sprinkled arbitrarily and finally they are placed in prescheduled zones by dividing a deployment field into a number of practical professional zones. Replica detection schemes which s used in the previous one can be easily detect replicas in a network based on the final arrangement because they require only a node ID and a node in the final also has a node ID. Hence the replica detection strategy used in the previous one cannot find out the replicas in the former. Basically the network information is defined before node consumption. The proposed solution allows or find out the replicas based on the random uniform consumption, which can detect replicas in spite of of the consumption strategies.

The Wireless Sensor Networks (WSNs) are frequently deployed in hostile environments where an opponent can physically gain the control over some of the sensor nodes and then firstly reprogram it by using original nodes secret information and then replicate them in a large number of clones. After that they can easily charming the control over the WSN. Some of the distributed solutions to concentrate on this primary problem have been freshly proposed. On the other hand, these solutions are not acceptable. Firstly, they are energy and memory challenging and are the main and serious drawback for any protocol to be used in the WSN-resource controlled environment. Additionally they are vulnerable to the specific adversary models introduced in this paper. The donations of this work are threefold. First one is to analyze the attractive properties of a dispersed mechanism for the detection of sensor nodes in the replication attacks. Second one is, it shows that the well known solutions for this problem do not completely meet requirements. And the last one is the proposing a new self-healing, Randomized, Efficient, and Distributed (RED) protocol for the detection of node replication attacks, and shows that it satisfies the introduced requirements. Finally, widespread simulations show that proposed protocol is highly efficient in communication and computation; is much more effective than challenging solutions in the literature; and is opposed to the new kind of attacks introduced in this paper, while the other already introduced solutions are not.

The sensor nodes that are deployed in hostile environments are vulnerable to capture and cooperation. An opponent may obtain private information from these sensors and then easily make clone from it and cleverly position them in the network to launch a diversity of insider attacks. This kind of attack process is generally called as a clone attack. Presently, the defenses against clone attacks are not only very few, but also suffer from selective intermission of detection and high overhead. This paper, propose a new effective and efficient scheme, called SET to detect such clone attacks. The key idea behind of this SET is to sense clones by computing the set operations of exclusive subsets in the network. Firstly the SET securely forms restricted unit subsets among one-hop neighbors in the WSN in a distributed way. This secure subset formation also provides the authentication of nodes' subset membership. After that, the SET then employs a tree structure to compute non-overlapped set operations and integrates interleaved substantiation to prevent unauthorized falsification of subset information during forwarding. The randomization is used to make further the exclusive subset and tree formation changeable to a challenger. We show the reliability and resilience of SET by analyzing the probability that an adversary may effectively obstruct the set operations. Performance analysis and simulations also demonstrate that the projected scheme is more efficient than existing schemes from both communication and memory cost standpoints.

The WSN's are defenseless to the duplicate nodes or clone's attack, because of cost is less, resource controlled sensor nodes, and uncontrolled environments where they are left unattended. There are no. of distributed protocols have been projected for detecting the duplicate node or clone. On the other hand, some of the protocols rely on an implied assumption that every node is aware of all other nodes' existence. Other protocols using a geographic hash table require that nodes know the general network deployment graph. Those considerations are hardly holding for many sensor networks. This paper present a novel node clone detection protocol based on Distributed Hash Table (DHT). The DHT provides a good distributed properties and this protocol is practical for every kind of sensor networks. This projected protocol analyzes the protocol performance theoretically. Furthermore, this paper implements protocol in the OMNeT++ simulation framework. The widespread simulation results of this shows that the projected protocol can be detect clone professionally and holds strong confrontation next to adversaries.

III. SYSTEM ARCHITECTURE

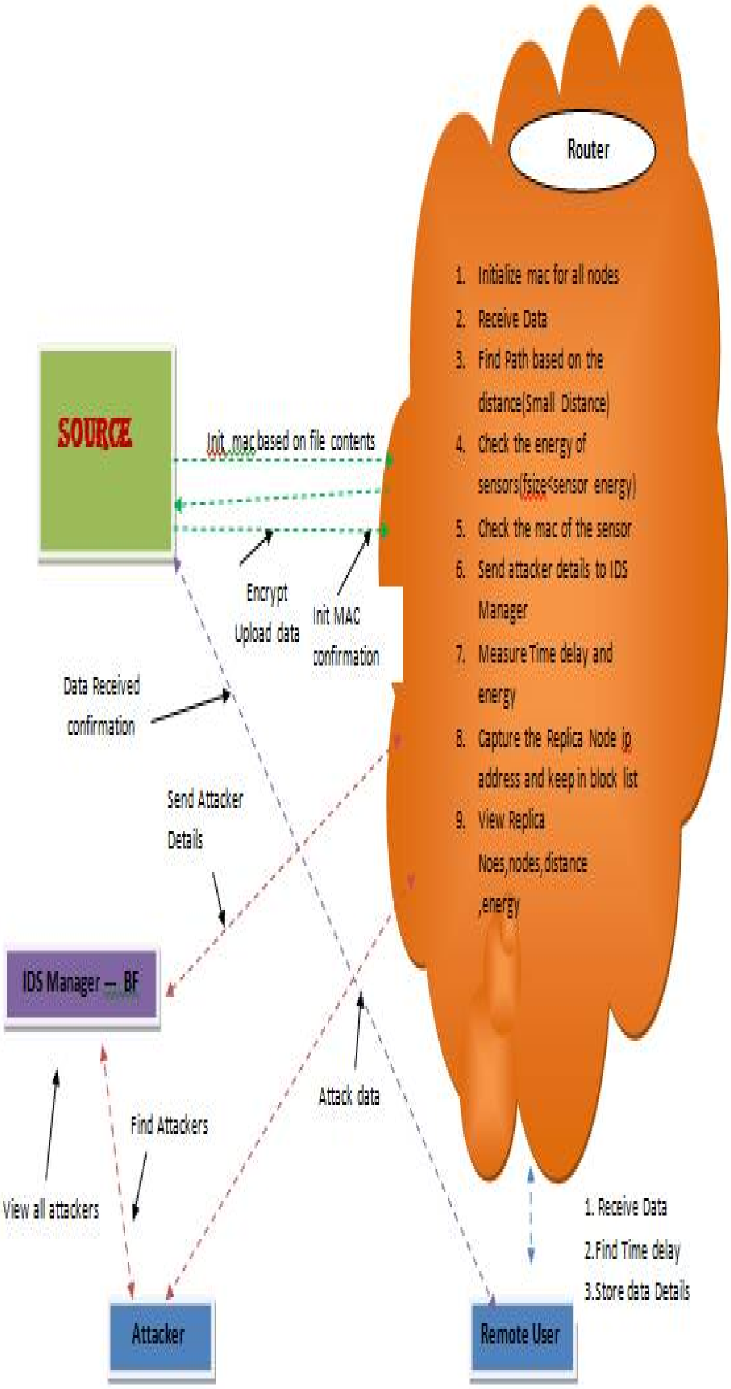

Router
1. Initialize mac for all nodes
2. Receive Data
3. Find Path based on the distance(Small Distance)
4. Check the energy of sensors(fsize<sensor energy)
5. Check the mac of the sensor
6. Send attacker details to IDS Manager
7. Measure Time delay and energy
8. Capture the Replica Node ip address and keep in block list
9. View Replica Noes,nodes,distance ,energy
SOURCE
Init mac based on file contents
Encrypt
Upload data
Init MAC
confirmation
Data Received
confirmation
Send Attacker
Details
IDS Manager – BF
View all attackers
Find Attackers
Attack data
Attacker
Remote User
1. Receive Data
2.Find Time delay
3.Store data Details

Fig 1: System Architecture

Sensor networks are usually designed and deployed for a specific application. They are scalable with a minimal effort. Network topology changes frequently in WSN due to energy depletion, channel fading, node failure and damage. Sensor nodes are self-configurable and they are densely deployed in the target area. Battery is the only source of energy for most of the sensing devices. Most of the applications of WSN are data centric and the data-flows within the network obey many-to-one traffic pattern. Due to higher node density, data redundancy may exist in the network.

IV. MODULE

Service Provider:

In this module, the Service Provider browses the required file, initializes nodes with digital signature and uploads to the end user (node a, node b, node c, node d, node e, node f) via Router.

Router:

The Router is responsible for forwarding the data file in shortest distance to the destination; the Router consists of Group of nodes, the each and every node (n1, n2, n3, n4, n5, n6, n7, n8, n8, n10, n11, n12, n13) consist of Bandwidth and Digital Signature. If router had found any malicious or traffic node in the router then it forwards to the IDS Manager. In Router we can assign the bandwidth for the nodes and can view the node details with their tags Node Name, Sender IP, Injected data, Digital Signature, Bandwidth and status.

IDS Manger (Bloom Filter):

The IDS manager is nothing but Intrusion Detection System manager and which is responsible to filter the malevolent data and traffic data. The IDS manager decides the phases based on Router status and then conclude depending on the two phases i.e. the “Training Phase” and the “Test Phase”.

Training Phase:

The “Normal Profile Generation” module is making operational in the Training Phase to produce a profiles for the various types of justifiable traffic records, and the generated normal profiles are stored in a database.

Test Phase:

The “Tested Profile Generation” module is used in the Test Phase to build profiles for individual observed traffic records. Then, the tested profiles are handed over to the Attack Detection module, which compares the individual tested profiles with the particular stored normal profiles.

End User

In this module, the End user can receive the data file from the Service Provider which is sent via Router, if malicious or traffic node is found in the router then it forwards to the IDS Manager to filter the content and adds to the Replica Node profile.

Forgery Replica Node and Packet Droppers

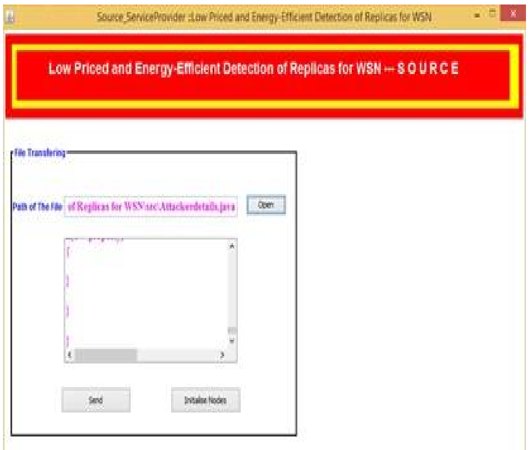
In this module, the malicious node or the traffic node details can be identified by a threshold-based classifier is employed in the Attack Detection module to differentiate DoS attacks from genuine traffic. The Replica Node can inject the fake message and generates the signature to a particular node in the router with the help of threshold-based classifier in testing phase and then adds to the Replica Node profile.

Advantage:

- The strategy disperses traffic over the entire network, resulting in small packet loss and considerable energy saving.
- We show that the proposed solution provides a high detection ratio as well as short detection time for detecting replicas without the use of GPS, as com-pared to existing schemes.
- The proposed solution is more energy-efficient than existing schemes

DOI: 10.15680/IJIRCCE.2016. 0406364

V. EXPERIMENTAL RESULT

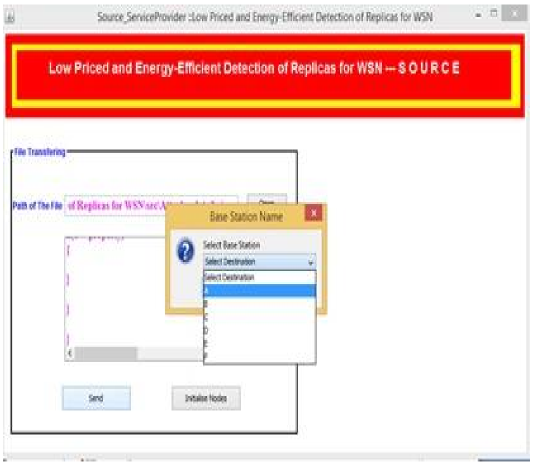


Source_ServiceProvider :Low Priced and Energy-Efficient Detection of Replicas for WSN

Low Priced and Energy-Efficient Detection of Replicas for WSN --- S O U R C E

Path of The File: of Replicas for WSN\src\Attackerdetails.java

Fig 2: Home Page



Source_ServiceProvider :Low Priced and Energy-Efficient Detection of Replicas for WSN

Low Priced and Energy-Efficient Detection of Replicas for WSN --- S O U R C E

Path of The File: of Replicas for WSN\src\A

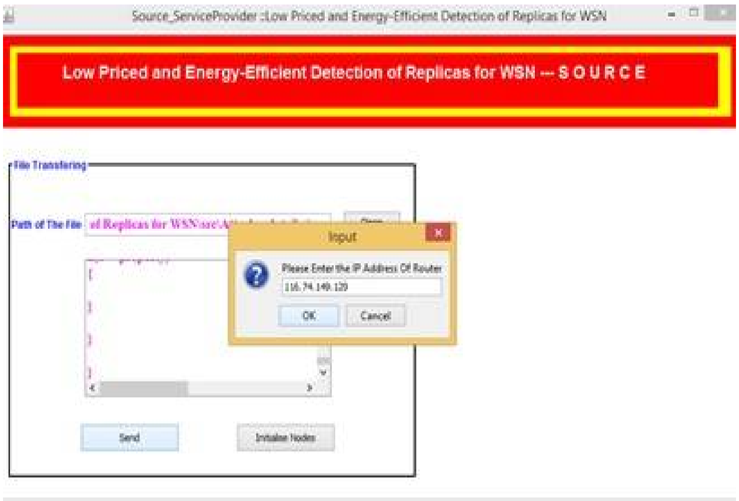
Base Station Name

Select Base Station

Select Destination

Select Destination
A
B
C
D
E
F

Fig 3: Selection Path



Source_ServiceProvider :Low Priced and Energy-Efficient Detection of Replicas for WSN

Low Priced and Energy-Efficient Detection of Replicas for WSN --- S O U R C E

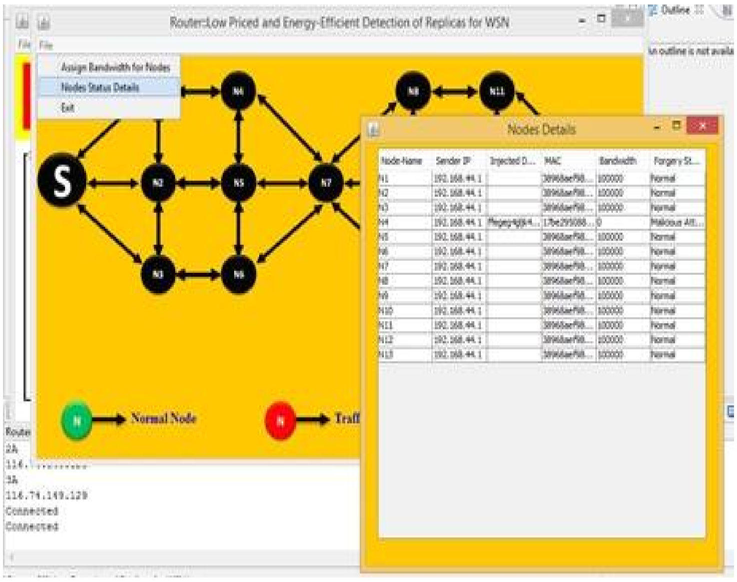
Path of The File: of Replicas for WSN\src\A

Input

Please Enter the IP Address Of Router

116.74.149.120

Fig 4: IP Address of Router



Router
2A
116.........
3A
116.74.149.129
Connected
Connected

Nodes Details

Node-Name	Sender IP	Injected D...	MAC	Bandwidth	Forgery St...
N1	192.168.44.1		38968aef98...	100000	Normal
N2	192.168.44.1		38968aef98...	100000	Normal
N3	192.168.44.1		38968aef98...	100000	Normal
N4	192.168.44.1	ffegeg4gjj4...	17be295088...	0	Malicious Att...
N5	192.168.44.1		38968aef98...	100000	Normal
N6	192.168.44.1		38968aef98...	100000	Normal
N7	192.168.44.1		38968aef98...	100000	Normal
N8	192.168.44.1		38968aef98...	100000	Normal
N9	192.168.44.1		38968aef98...	100000	Normal
N10	192.168.44.1		38968aef98...	100000	Normal
N11	192.168.44.1		38968aef98...	100000	Normal
N12	192.168.44.1		38968aef98...	100000	Normal
N13	192.168.44.1		38968aef98...	100000	Normal

Fig 5: Node Details

VI. CONCLUSION

This paper proposed a low priced and energy-efficient way or strategy to detect duplicate node for static wireless sensor network. Projected system does not use any additional hardware; where existing system need of expensive hardware like as GPS. Proposed solution use exhibits duplicate node or good performance than existing scheme. When one or more replicas detect within the short time frame; then it's automatically increase the performance of the system by achieving the also energy efficiency.

This paper concludes that the duplicates nodes in Wireless sensor networks are detected by using a new Static testing technique called sequential probability. Using this technique the settlement made with the sensor nodes. Nodes are detected efficiently in mobile sensor networks also.

ACKNOWLEDGMENT

I want to thank all people who help me in different way. Especially I am thankful to my guide "**Prof. Bere S.S"** for him continuous support and guidance in my work. Also, I would like thank our PG coordinator **"Prof. Priyadarshi Amrit"**. Lastly, I thank to "**IPGCON-16"** who have given opportunity to present my paper.

REFERENCES

[1] K. Cho, B. Lee, and D. Hoon Lee, "Low-Priced and Energy-Efficient Detection of Replicas for Wireless Sensor Networks'09: IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 11, NO. 5, SEPTEMBER/OCTOBER 2014.
[2] C.P. Mayer, "Security and Privacy Challenges in the Internet of Things," Electronic Comm. EASST, vol. 17, pp. 1-12, 2009.
[3] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Survey Internet of Things: Vision, Applications and Research Challenges," J. Ad Hoc Networks, vol. 10, no. 7, pp. 1497-1516, Sept. 2012.
[4] B. Parno, A. Perrig, and V. Gligor, "Distributed Detection of Node Replication Attacks in Sensor Networks," Proc. IEEE Symp. Security and Privacy, pp. 49-63, 2005.
[5] M. Conti, R.D. Pietro, L. Mancini, and A. Mei, "Distributed Detection of Clone Attacks in Wireless Sensor Networks," IEEE Trans. Dependable and Secure Computing, vol. 8, no. 5, pp. 685-698, Sept. 2011.
[6] C.A. Melchor, B. Ait-Salem, and P. Gaborit, "Active Detection of Node Replication Attacks," Int'l J. Computer Science and Network Security, vol. 9, no. 2, pp. 13-21, 2009.
[7] H. Choi, S. Zhu, and T.F.L. Porta, "Set: Detecting Node Clones in Sensor Networks," Proc. Third Int'l Conf. Security and Privacy in Comm. Networks and the Workshops (SecureComm '07), pp. 341-350, 2007.
[8] Z. Li and G. Gong, "DHT-Based Detection of Node Clone in Wireless Sensor Networks," Proc. First Int'l Conf. Adhoc Networks, pp. 240-255, 2009.

[9] K. Xing, F. Liu, X. Cheng, and D.H.C. Du, “Real-Time Detection of Clone Attacks in Wireless Sensor Networks,” Proc. 28th Int’l Conf. Distributed Computing Systems (ICDCS ’07), pp. 3-10, 2008.

[10] Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, “Random-Walk Based Approach to Detect Clone Attacks in Wireless Sensor Networks,” IEEE J. Selected Areas Comm., vol. 28, no. 5, pp. 677-691, June 2010.

[11] B. Zhu, S. Setia, S. Jajodia, S. Roy, and L. Wang, “Localized Multicast: Efficient and Distributed Replica Detection in Large-Scale Sensor Networks,” IEEE Trans. Mobile Computing, vol. 9, no. 7, pp. 913-926, July 2010.

[12] J.-W. Ho, D. Liu, M. Wright, and S.K. Das, “Distributed Detection of Replica Node Attacks with Group Deployment Knowledge in Wireless Sensor Networks,” J. Ad Hoc Networks, vol. 7, no. 8, pp. 1476-1488, Nov. 2009.

[13] C.-M. Yu, C.-S. Lu, and S.-Y. Kuo, “Mobile Sensor Network Resilient against Node Replication Attacks,” Proc. Fifth Ann. IEEE Comm. Society Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON ’08), pp. 597-599, June 2008.

[14] C.-M. Yu, C.-S. Lu, and S.-Y. Kuo, “Efficient and Distributed Detection of Node Replication Attacks in Mobile Sensor Networks,” Proc. IEEE 70th Vehicular Technology Conf. Fall (VTC 2009-Fall), pp. 1-5, Sept. 2009.

[15] J.-W. Ho, M. Wright, and S. Das, “Fast Detection of Replica Node Attacks in Mobile Sensor Networks Using Sequential Analysis,” Proc. IEEE INFOCOM, pp. 1773-1781, Apr. 2009.

[16] K. Cho, M. Jo, and D.H. Lee, “Effective Distributed Detection of Clones in Mobile Wireless Sensor Networks,” Proc. Int’l Conf. Internet (ICONI), pp. 299-304, Dec. 2009.

[17] K. Xing and X. Cheng, “From Time Domain to Space Domain: Detecting Replica Attacks in Mobile Ad Hoc Networks,” Proc. INFOCOM, pp. 1595-1603, 2010.

[18] J.-W. Ho, M. Wright, and S.K. Das, “Distributed Detection of Mobile Malicious Node Attacks in Wireless Sensor Networks,” J. Ad Hoc Networks, vol. 10, no. 3, pp. 512-523, May 2012.

[19] K. Cho, M. Jo, T. Kwon, H.-H. Chen, and D.H. Lee, “Classification and Experimental Analysis for Clone Detection Approaches in Wireless Sensor Networks,” IEEE Systems J., vol. 7, no. 1, pp. 26- 35, Mar. 2013.

[20] J.-W. Ho, M. Wright, and S.K. Das, “Zonetrust: Fast Zone-Based Node Compromise Detection and Revocation in Wireless Sensor Networks Using Sequential Hypothesis Testing,” IEEE Trans. Dependable and Secure Computing, vol. 9, no. 4, pp. 494-510, July- Aug. 2012.