International Journal of Computer Networks and Communications Security

VOL. 2, NO. 7, JULY 2014, 225–231
Available online at: www.ijcncs.org
ISSN 2308-9830

MadCD: A Mobile Agent Based Distributed Clone Detection Method in Mobile WSNs

SEPIDE MORADI[1] and MINA ZOLFY LIGHVAN[2]

[1, 2] Department of Electrical and Computer Engineering, Tabriz University, Tabriz, Iran

E-mail: [1]s.moradi91@ms.tabrizu.ac.ir [2]mzolfy@tabrizu.ac.ir

ABSTRACT

Sensor nodes used in enemy environments are disposed to capture and Compromise. An adversary may obtain secret information from sensors, such attack is named as clone attack. The clone attack, Replicate nodes and arrange them in the network to launch a variety of other attacks. In recent years, mobile agents have been suggested for effective data broadcasting in sensor networks and a number of researchists use mobile agents as a novel template for distributed purpose to dominate the limitations of sensor nodes. Recently, several solutions are proposed to tackle clone attacks, but they mostly suffer from high overhead. In this paper the Macdc method is proposed to encounter the replication attacks using mobile agent technology in mobile WSNs. The mobile agents are used to aware every node from its trustworthy neighbors, so nodes do not interact with malicious nodes. The analysis and simulation results prove the effectiveness and efficiency of proposed Macdc method which also reduces the comparisons overhead.

Keywords: *Wireless sensor networks, Clone attack, Clone detection, Mobile agent, location.*

1 INTRODUCTION

Wireless sensor networks are gradually becomes a proper solution for a wide area of real world monitoring problems. These networks are typically organized in uncontrollable and usually not reliable environments. Almost all sensor networks are physically reachable and thus more vulnerable. An attacker may capture and compromise a node and control a valid member of the network.

The clone attack is the basis of a range of attacks. A clone can make a black hole and wormhole attack [1]. The clone attack can threat a network because of the two points mentioned below; i) a clone is considered honest by its neighbors. In fact, without global countermeasures, trust nodes cannot be aware of the actuality that they have a clone between their neighbors. ii) A single adversary node is enough to have a large amount of compromised nodes [2]. An attack inconsiderately alike to the node replication attack is the Sybil attack[3]. Where one physical sensor node gains an unfair benefit by claiming several ids. Therefore security becomes a serious problem WSNs.

The work presented in this is paper focus on the security of WSNs with proposing a method to detect clone attacks in this networks. The organization of the rest of the paper is as follow: In section 2 we provide a short text containing some background information. In section 3 explained various proposed solutions for detecting clone attacks. In section 4 we discuss the System assumptions. In Section 5 we present our Clone attack detection method. In Section 5.4 we discuss analyze of our solution overhead. Finally, in Section 1 we give our conclusion.

2 BACKGROUND

2.1 Wireless Sensor Network

A Wireless Sensor Network (WSN) is compromise a large number sensor nodes deployed over a wide area that is used for sensing and observing various phenomena. Wireless sensors consist of low cost hardware components, with limited power, communication, and memory resources. WSN consists of static and mobile sensor.

2.2 Security

The security of WSNs is one of their critical issues. Once sensor nodes have been deployed in the area of interest, there will be minimal human involvement and observation. This can be difficult when the WSN is deployed in enemy environments. In such environments nodes are vulnerable to physical attacks. One of the important physical attacks is the insertion of cloned nodes into WSNs.

2.3 Clone attack

Replicated nodes, although organized by the adversary, will be recognized as authentic members of the network because they carry all cryptographic secrets extracted from captured node. Such attacks are actual hazardous because they enable the attacker to leverage the compromise of a limited number of nodes to apply control over a great part of the network.

2.4 Mobile Agent

An agent is fragment of a program that are self-control and can move from one node to another node. In addition to data transfer, an agent can compute. Distributed systems are suitable environments for applications based on agent and agent mobiles are essentially effective for dynamic network environments. Mobile agents can be used to lessening the communication cost, especially over low bandwidth links such as sensor networks, by moving the processing function to the data rather than bringing the data to a central processor [4]. These features make them more suitable for WSNs.

3 RELATED WORK

Clone detection methods can be classified based on two criteria. In the classification based on the nodes mobility two categories are the methods used in static WSNs and the method used in mobile WSNs. In the other classification methods are categorized into centralized and distributed approaches. The focus of this work is on the distributed clone detection in mobile Wireless Sensor Networks.

XED[5] is a protocol based on conflict, in which when the nodes ni and node nj can meet each other, both of them produce a random number(rni and rnj respectively) and exchange them. Then the nodes store both received and sent numbers. If ni and nj meet again later, they swap the previously stored numbers and compare it with the numbers stored before and based on the comparison result can detect the attack [6].

In a clone attack the clone node must be replicated. To replicate such a node first it should be separated from the network and then its information must be extracted. This information extraction take some times and The SDD [7] procedure use that time period for detecting the clone attack. The detection capability of SDD is not high enough and to improve that, CDD [7] procedure has been submitted. The CDD takes advantages of nodes cooperation to increase the clone node capture detection rate. In CDD, node-exchanging information happens just when they are in the same communication radius. This method increases the detection probability; but increases the communication overhead and memory either.

In UTLTSE [8] when a witness node recognize a clone node in time-location assertion instead of broad casting the assertion all over the network, only exchange it when the meet other witness nodes.

In SHD [9], Each node sends a message to all nodes in its frequency range. This message contains the senders' id and the list of its neighbors. HOP and HIP [10] are two other protocol proposed for clone attack detection. In HIP each node compares its location with the location of its neighbors. In HOP each node contain a history of previously met nodes and in this methods the nodes compare the histories with each other. In HIP and HOP any inconsistency in the location of a node shows that the node is a Clone.

4 SYSTEM ASSUMPTIONS

In this section and the corresponding subsections the elementary Assumptions of the network model and the Threat model in Macdc method are described.

4.1 Network model

The WSN is composed of n sensor nodes and the nodes are arbitrarily deployed in a 200 × 200 square meter area. The node mobility is modeled according to a random waypoint algorithm [11] with the speed of 10 m/s. In RWP each node selects a random destination in the network area and then moves to this selected destination. After arriving at the desired destination, the node waits for a short random time and then repeat the movement. This behavior is repeated for the lifetime of the network[12]. Each node has a communication radius of R. The WSN contain only one base station which is statically placed in the field center (200,200) and has infinite energy. The nodes know

their own location (using GPS or the protocol of [13]). The mobile agents are placed randomly on nodes and their cycling process is repeated once per each 5-10 s. Because of using single hop communications no routing protocol is required [10]. Consequently the method does not need to store routing information.

Table 1. Notation

Parameter	Value
n	Number of nodes in the network
R	Communication radius of a node
C	Number of cloned Nodes
h	History log length(a protocol parameter)
d	Numbers of neighbor

4.2 Threat model

The threat model called persistent adversary, introduced in[10] is used. In this model C randomly selected sensors are cloned and keep their control over the network for the whole life time of the network. A clone node can put false assertions in the network.

5 PROPOSED APPROACH

This section focuses on the proposed method which uses the mobile agents for improving the security of the WSN. The mobile agents are used to inform the existence of malicious nodes to the regular nodes and prevent them of listening to the traffics and fake information generated by those malicious nodes [14].

5.1 Agent design

Different from some other methods [15], we just use one kind of agent, and agents only interact with the node which is staying on [16]. We assumes agent node are reliable.

5.2 Agent packet

Table 2shows an object instantiated from agent packet. The agent program contains a compare function (same as the HOP and HIP, introduced in [10]) that is used for detecting the clone attack in the network As mentioned before, each node tries to go under the cover of an agent.

The srcId and dstId fields are used for storing the source and destination ids in an agent migration.(moving of an agent from an agent node to a single hop neighbor node and reversal to its base node is called migration [16]), respectively. The data part contains trustbit and agentbit fields. The trustbit is used for determining trust neighbors and the agentbit indicates that the node is agent or not. The Datacode is used to encipher data and insure the accuracy of the data part in the agent packet. If the agent authenticate a node as a trustable node, Datacode will be given to the node then the node can extract accurate data from agent packet [16].

Table 2. Object Agent Packets

Agent Packet
-srcId *-stId* *-Datacode* *-data*
+Compare()

5.3 Node memory structure:

A table called ‘neighbor matrix’ is placed in node memory which retains single hop neighbors of that node. The Id, trustbit and agentbit are information stored in neighbor matrix. The Id is the Id number of a single hop neighbor node. trustbit and agentbit are as introduced in subsection 5.2. In this paper valid nodes don’t interact with malicious nodes and exchange data only with the trusted nodes. [16].

5.4 Algorithm

The proposed method is executed in “network organization stage” and “network conversation stage” which are described below.

5.5 Network organization stage

In this stage nodes are uniformly located in the network. The base station chooses some of the nodes for sending the agent packets to them. The nodes that take an agent packet from the base station are known as agent node. Agent nodes are trust.

5.6 Network conversation stage

This method is executed in several rounds. For each protocol round, every node broadcast HELLO packets to build the neighbor matrix and find neighbors within communication range. Malicious nodes can simply put themselves into neighbor matrix. After finding neighbors, each entry of neighbor matrix contains the ids of single hop neighbor nodes but still the agentbit and trustbit are false[16]. Every sensor store a log history (containing neighbor’s id and location in a round) of the neighbors met before. After collecting logs,

each node ni sends a message Msg (introduced in [10] which contain its id and location node and also it's log history collected until now) to agent node that is within communication domain of ni. In this case, each agent node, have a list (msglist) of Mgs received from its neighbors. Before any data exchange, the agent will compare the received messages. When a node with the same id is found in two position in a single round, it will be known as replica and related trustbit of the node in the neighbor matrix will become false. After the determination of neighbors' legitimacy, agent nodes multicast a packet named 'trust matrix' to all its trustable not agent neighbors [16].

Algorithm 1 shows the pseudo code of proposed method algorithm.

Algorithm 1

Agents **← Generate agent nodes;**
while (true)
For all nodes in WSN
Select node n_i
Find n_i **neighbors**
Update *neighbor matrix*
Construct the *Msg* **message**
Send the *Msg* **message to the nearest agent node**
Update *msglist* **in receiver agent nodes**
For all nodes in *Agents*
Select node ag_i
Compare messages in *msglist* **of** ag_i **with each other**
Detect clone nodes based on comparison
Update *neighbor matrix*
Broadcast ***trust-matrix***

5.7. Detection overhead

This section focuses on the computation costs required for clone detection. The average number of sensor's locations that are sent and received for clone detection, determines the mentioned computation cost. Every node send h+1 (h is the size of history) locations and each agent node receive a history log with size of (h+1)d from d neighbors, on average, per round. Therefore average receiving cost per agent nodes is O(d2h) and average sending cost per regular nodes (not agent) is O(d (h+1)). The total cost for all Rounds is O((dh)2) comparisons. The simulation based result for the data illustrated in the previous paragraph are explained in the subsection 1.1.

6 EXPERIMENTAL RESULT

For analyzing Macdc method and comparing this method with other works, the method is simulated using .Net Framework technology and C#.NET programming language. The WSN simulator of [16] is used for this method. The simulation results are evaluated based on the energy consumption and the number of performed comparisons. Table 3.Simulation Parameters indicates parameters used in this simulation.

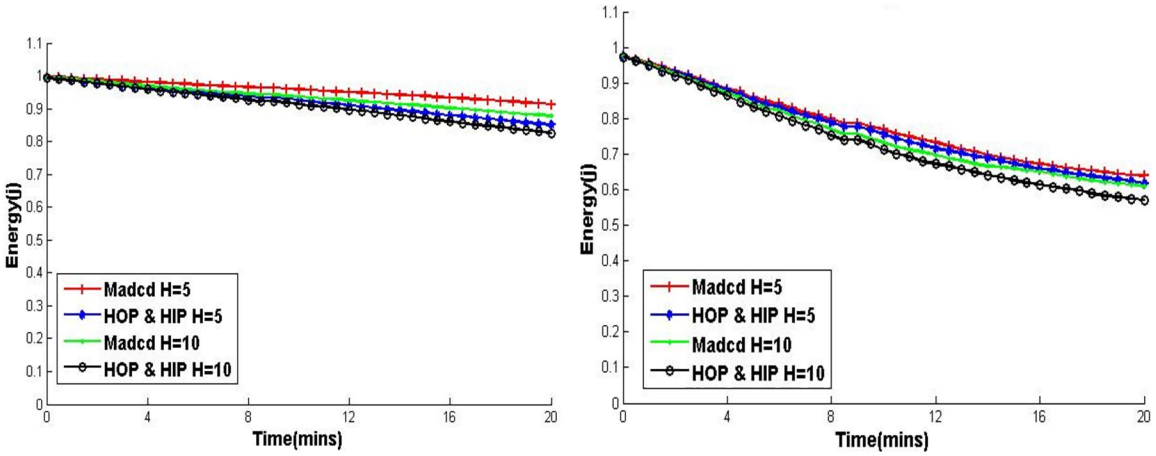
The test bed network is constructed and simulated 40 times. In 20 experiments the networks are constructed with 100 nodes and in the other 20 experiments the networks are constructed with 200 nodes. In each simulation run, a single node is selected randomly as the clone. In all experiments 10 percent of nodes are selected as the agent nodes. Energy in wireless sensor networks is a critical issue, to estimate the expended energy in sensor nodes, Heinzelman [17] energy model has been applied in our method.

Table 3.Simulation Parameters

Symbol	Meaning
Network scale	200 m*200 m
Transmission range	50 m
Energy	1 J
Speed	10 m/s

6.1 Energy Composition

Figure 1 shows, the energy consumption obtained from the simulation result. The results shows that in comparison to the other methods[10], the energy consumption of the method presented in this paper is less than the others.

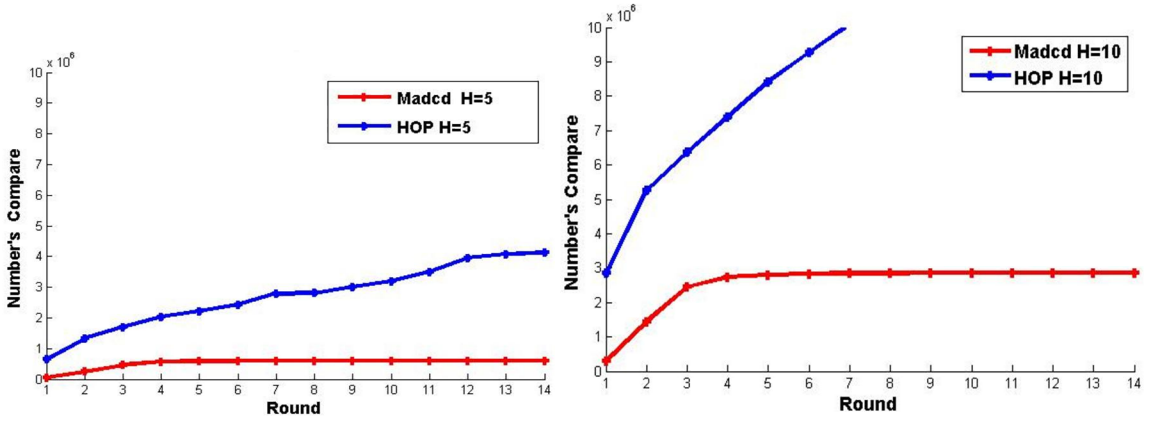


(a) *(b)*

Figure 1. The average consumed energy in the network (a) with n=100 node. (b) With n=200 node.

6.2 Cost Comparison

Number of required comparisons for detecting replica, per round, (with n=100) is shown in. In contrast to the method presented in [10], in which every node compares all of its neighbor's location with each other, in Macdc just agent nodes do this comparison task. Thus, the number of performed comparisons is reduced in the presented method.



(a) *(b)*

Fig. 2. Number average of comparison cost for (a) h=5 and (b) h=10.

7 CONCLUSION

In this paper, a novel idea for detecting replica in the mobile WSNs is presented. The presented Macdc method takes advantages of history logs collected via agent nodes to delete the replica node. The replica node deleting is performed through assigning the trustbit of that node in the neighbor matrix, equal to false. The agents are some programming codes for finding trusted neighbors based on the HIP model and the HOP model, hence the secured routes are established. In each round, the regular nodes collect information from all of its neighbors and send it to the corresponding agent node in order to find inconsistent information. This method does not suffer from false positives. Simulation analysis shows that there are improvement in terms of energy consumption, memory overhead compared to other methods [10] while both have similar detection rates.

8 REFERENCES

[1] Yih-Chun, H., A. Perrig, and D.B. Johnson. Packet leashes: a defense against wormhole attacks in wireless networks. in INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies. 2003.

[2] Conti, M., et al., Distributed Detection of Clone Attacks in Wireless Sensor Networks. Dependable and Secure Computing, IEEE Transactions on, 2011. 8(5): p. 685-698.

[3] Douceur, J.R., The Sybil Attack, in Revised Papers from the First International Workshop on Peer-to-Peer Systems. 2002, Springer-Verlag. p. 251-260.

[4] Chen, M., et al., Mobile Agent Based Wireless Sensor Networks. JOURNAL OF COMPUTERS, 2006. 1.

[5] Chia-Mu, Y., L. Chun-Shien, and K. Sy-Yen. Mobile Sensor Network Resilient Against Node Replication Attacks. in Sensor, Mesh and Ad Hoc Communications and Networks, 2008. SECON '08. 5th Annual IEEE Communications Society Conference on. 2008.

[6] Ansari, M.H. and V.T. Vakili, Performance Analysis and Classification of Clone Attack Detection Procedures in Mobile Wireless Sensor Networks. International Journal of Computer Applications, 2013. 71: p. 5-12.

[7] Conti, M., et al., Emergent properties: detection of the node-capture attack in mobile wireless sensor networks, in Proceedings of the first ACM conference on Wireless network security. 2008, ACM: Alexandria, VA, USA. p. 214-219.

[8] Xiaoming, D., X. Yan, and C. Depin. MoBility-Assisted Detection Of The Replication attacks in mobile wireless sensor networks. in Wireless and Mobile Computing, Networking and Communications (WiMob), 2010 IEEE 6th International Conference on. 2010.

[9] Lou, Y., Y. Zhang, and S. Liu, Single Hop Detection of Node Clone Attacks in Mobile Wireless Sensor Networks. Procedia Engineering, 2012. 29(0): p. 2798-2803.

[10] Conti, M., R. Di Pietro, and A. Spognardi, Clone wars: Distributed detection of clone attacks in mobile WSNs. Journal of Computer and System Sciences, 2014. 80(3): p. 654-669.

[11] Johnson, D. and D. Maltz, Dynamic Source Routing in Ad Hoc Wireless Networks, in Mobile Computing, T. Imielinski and H. Korth, Editors. 1996, Springer US. p. 153-181.

[12] Broch, J., et al., A performance comparison of multi-hop wireless ad hoc network routing protocols, in Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking. 1998, ACM: Dallas, Texas, USA. p. 85-97.

[13] Caruso, A., et al. GPS free coordinate assignment and routing in wireless sensor networks. in INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE. 2005.

[14] Brar, R.S. and H. Arora, Mobile Agent Security issue in Wireless Sensor Networks. International Journal of Advanced Research in Computer Science and Software Engineering, 2013. 3(1): p. 378-81.

[15] Stafrace, S.K. and N. Antonopoulos, Military tactics in agent-based sinkhole attack detection for wireless ad hoc networks. Computer Communications, 2010. 33(5): p. 619-638.

[16] Hamedheidari, S. and R. Rafeh, A novel agent-based approach to detect sinkhole attacks in wireless sensor networks. Computers & Security, 2013. 37(0): p. 1-14.

[17] Heinzelman, W., Application-specific protocol architectures for wireless networks. 2000, Massachusetts Institute of Technology.

AUTHOR PROFILES:

Sepide Moradi received the B.S.c degree in Computer Engineering (Software) from Payam Noor University, Hamadan, Iran in 2012. She is currently M.Sc. student in Computer Engineering (Software) from Electrical and Computer Engineering faculty of Tabriz University, Iran. Her research interests include network, security, and Intrusion Detection Systems, Object oriented Programming & Design.

Mina Zolfy Lighvan received the B.S.c degree in Computer Engineering (hardware) and M.Sc. degree in Computer Engineering (Computer Architecture) from ECE faculty, university of Tehran, Iran in 1999, 2002 respectively. She received Ph.D. degree in Electronic Engineering

(Digital Electronic) from Electrical and Computer Engineering faculty of Tabriz University, Iran. She currently is an assistant professor and works as a lecturer in Tabriz university. She has more than 20 papers that were published in different national and international conferences and Journals. Dr. Zolfy major research interests include Text Retrieval, Object oriented Programming & Design, Algorithms Analysis, HDL Simulation, HDL Verification, HDL Fault Simulation, HDL Test Tool VHDL, Verilog, hardware test, CAD Tool, synthesis, Digital circuit design & simulation.