On The Node Clone Detection Using DHT and RDE

[1]S.Sathiya, [2]K.Suganthi, [3]S.Venkatesh
[123]Department of Information Technology, S.K.P Engineering College, Tiruvannamalai.
[3] Assistant professor, Department of IT, S.K.P Engineering College, Tiruvannamalai.
[1] sathiyaselvamit@gmail.com, [2] mksugu21@gmail.com, [3] venkat.it.vk@gmail.com

***Abstract* - A wireless sensor network is a collection of nodes organized in to a cooperative network. This network is prone to various attacks due to poor security. In this paper, we propose two novel node clone detection protocols. The first one is based on a distributed hash table (DHT), which is fully decentralized, key-based caching and checking system is constructed to catch cloned nodes effectively. Our second distributed detection protocol, named randomly directed exploration, presents good communication performance for dense sensor networks.**

***Index Terms*—Distributed hash table, node clone attack, randomly directed exploration; wireless sensor networks (WSNs).**

I. INTRODUCTION

Wireless sensor network, a network of sensor nodes, which are tiny with limited resources that communicate with each other to achieve a goal, through the wireless channels. This network is mainly used in military applications for monitoring security and in civil applications. This network is deployed in harsh and hostile environments. Based on operating nature, it is unattended and prone to various attacks. The basic security requirements of wireless sensor network are integrity, availability, confidentiality and communication. In this paper, we present two novel, practical node clone detection protocols with different tradeoffs on network conditions and performance. The first proposal is based on a distributed hash table (DHT) by which a fully decentralized, key-based caching and checking System is constructed to catch cloned nodes. The Protocol is efficient in storage consumption and high level security. Our second protocol, named Randomly directed exploration, is intended to provide highly efficient communication.

II. DETECTION PROTOCOLS

Based on the detection methodologies, we classify two novel node clone detection protocols.

1. Distributed hash table (DHT)
2. Randomly directed exploration (RDE)

A. Distributed hash table (DHT)

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

B. Randomly directed exploration (RDE)

This is intended to provide highly efficient communication performance with adequate detection probability for dense sensor networks. In the protocol, initially nodes send claiming messages containing a neighbor-list along with a maximum hop limit to randomly selected neighbors; then, 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 further reduce communication payload. During forwarding, intermediate nodes explore claiming messages for node clone detection. By design, this protocol consumes almost minimal memory, and the simulations show that it outperforms all other detection protocols in terms of communication cost, while the detection probability is satisfactory.

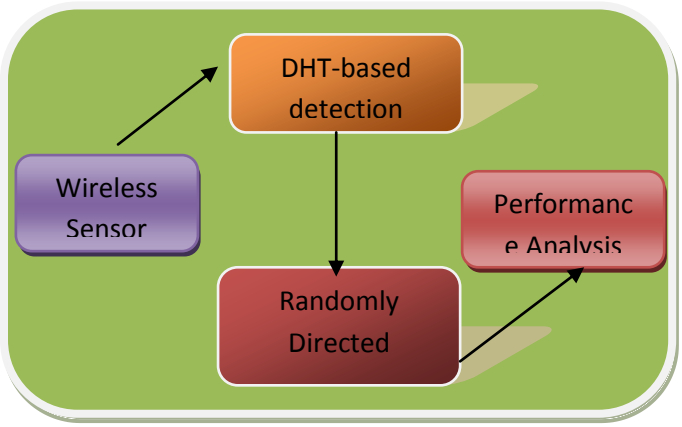

Fig 1: BLOCK DIAGRAM

III. EXISTING SYSTEM

WIRELESS sensor networks (WSNs) have gained a great deal of attention in the past decade due to their wide range of application areas and formidable design challenges. In general, wireless sensor networks consist of hundreds and thousands of low-cost, resource-constrained, distributed sensors nodes, which usually scatter in the surveillance area randomly, working without attendance. If the operation environment is hostile, security mechanisms against adversaries should be taken into consideration. Among many physical attacks to sensor networks, the node clone is a serious and dangerous one. Because of 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 credentials, and use those materials to clone many nodes out of off-the-shelf sensor hardware. Those cloned nodes that seem legitimate can freely join the sensor network and then significantly enlarge the adversary's capacities to manipulate the network maliciously.

DISADVANTAGES OF EXISTING SYSTEM

- Among many physical attacks to sensor networks, the node clone is a serious and dangerous one.
- Insufficient storage consumption performance in the existing system and low security level.

IV. PROPOSED SYSTEM

In this paper, we present two novel, practical node clone detection protocols with different tradeoffs on network conditions and performance. The first proposal is based on a distributed hash table (DHT) by which a fully decentralized, key-based caching and checking system is constructed to catch cloned nodes. The protocol's provides efficient memory consumption and a high level security and holds strong resistance against adversary's attacks. Our second protocol, named randomly directed exploration, is intended to provide highly efficient communication performance with adequate detection probability for dense sensor networks. In the protocol, initially nodes send claiming messages containing a neighbor-list along with a maximum hop limit to randomly selected neighbors; then, 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 further reduce communication payload. During forwarding, intermediate nodes explore claiming messages for node clone detection. By design, this protocol consumes almost minimal memory, and the simulations show that it outperforms all other detection protocols in terms of communication cost, while the detection probability is satisfactory.

Advantages of Proposed System

- The DHT-based protocol can detect node clone with high security level and holds strong resistance against adversary's attacks.
- Randomly directed exploration, is intended to provide highly efficient communication performance with adequate detection probability for dense sensor networks.

V. MODULES

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

VI. MODULES DESCRIPTION

A. Setting up Network Model

Our first module is setting up the network model. We consider a large-scale, homogeneous sensor network consisting of 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 our 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

B. Initialization Process

To activate all nodes 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.

C. Claiming neighbor's information

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

D. Processing claiming messages

A claiming message will be forwarded to its destination node via several Chord intermediate nodes. Only those nodes in the overlay

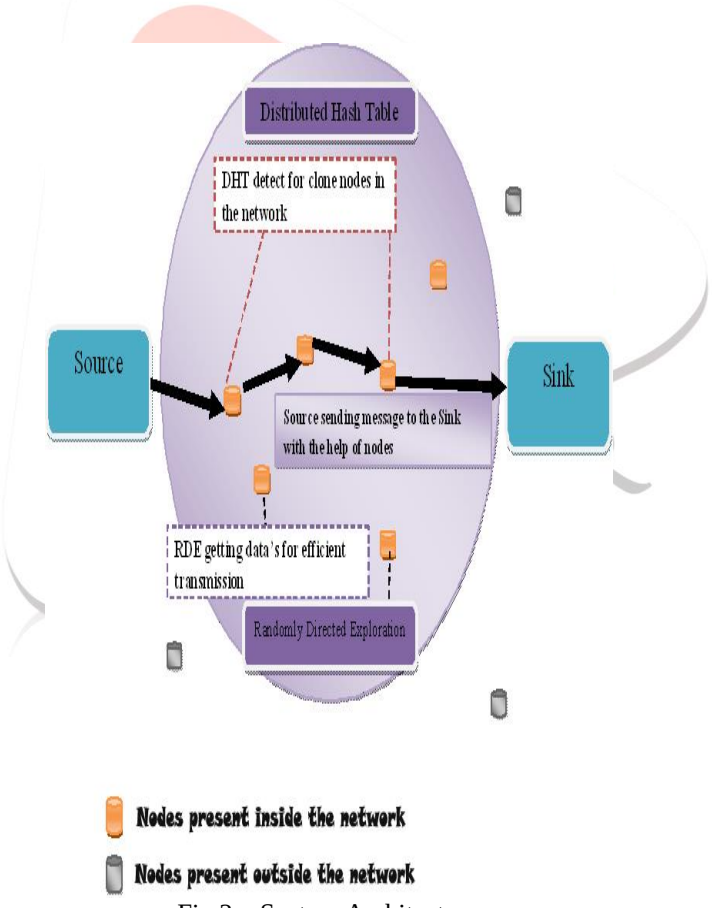

Fig 2: System Architecture

Intermediate nodes and the destination node) need to process a message, whereas 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, then the message has arrived at its destination. Otherwise, the message will be subsequently forwarded to the next node with the ID that is returned.

E. Sink Module

The sink is the point of contact for users of the sensor network. Each time the sink receives a question from a user, it first translates the question into multiple queries and then 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 from multiple storage nodes into the final answer and sends it back to the user.

F. Performance Analysis

For the DHT-based detection protocol, we use the following specific measurements to evaluate its performance:

- Average number of transmitted messages, representing the protocol's communication cost;
- Average size of node cache tables, standing for the protocol's storage consumption;
- Average number of witnesses, serving as the protocol's security level because the detection protocol is deterministic and symmetric.

VII. CONCLUSION

Sensor nodes lack tamper-resistant hardware and are subject to the node clone attack. In this paper, we present two distributed detection protocols: 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, and the other 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, the randomly directed exploration presents outstanding communication performance and minimal storage Consumption for dense sensor networks.

REFERENCES

[1] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in Proc. IEEE Symp. Security Privacy, 2005, pp. 49–63.
[2] H. Balakrishnan, M. F. Kaashoek, D. Karger, R. Morris, and I. Stoica, "Looking up data in P2P systems," Commun. ACM, vol. 46, no. 2, pp.43–48, 2003.
[3] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Location-based compromise tolerant security mechanisms for wireless sensor networks," IEEE J.Sel. Areas Commun. vol. 24, no. 2, pp. 247–260, Feb. 2006.
[4] S. Zhu, 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.
[5] R. Anderson, H. Chan, and A. Perrig, "Key infection: Smart trust for smart dust," in Proc. 12th IEEE ICNP, 2004, pp. 206–215.
[6] M. Conti, R. D. Pietro, L. V. Mancini, and A. Mei, "A randomized ,efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks," in Proc. 8thACMMobiHoc,Montreal,QC, Canada, 2007, pp. 80–89.
[7] B. Zhu, 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.
[8] H. Choi, S. Zhu, and T. F. La Porta, "SET: Detecting node clones insensor networks," in Proc. 3rd Secure Comm, 2007, pp. 341–350.
[9] R. Brooks, 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, pp. 1246–1258, Nov. 2007.
[10] L. Eschenauer 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.