ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 2, Issue 7, July 2015

On the Node Clone Detection in Wireless Sensor Networks

Gurramkondu Sunil Kumar[1], M. Naresh Babu[2]

PG Scholar, Dept of Computer Science, Vaagdevi Institute of Tech & Science, Proddatur, Kadapa, India[1]

Assistant Professor, Dept of Computer Science, Vaagdevi Institute of Tech & Science, Proddatur, Kadapa, India[2]

Abstract: Wireless sensor networks are vulnerable to the node clone, and several distributed protocols have been proposed to detect this attack. However, they require too strong assumptions to be practical for large-scale, randomly deployed sensor networks. In this paper, we propose two novel node clone detection protocols with different tradeoffs on network conditions and performance. The first one 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 effectively. The protocol performance on efficient storage consumption and high security level is theoretically deducted through a probability model, and the resulting equations, with necessary adjustments for real application, are supported by the simulations. Although the DHT-based protocol incurs similar communication cost as previous approaches, it may be considered a little high for some scenarios. To address this concern, our second distributed detection protocol, named randomly directed exploration, presents good communication performance for dense sensor networks, by a probabilistic directed forwarding technique along with random initial direction and border determination. The simulation results uphold the protocol design and show its efficiency on communication overhead and satisfactory detection probability.

Keywords: Wireless sensor networks, Distributed hash table, key-based caching, clone detection.

I. INTRODUCTION

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 sensor 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. For example, those vicious nodes occupy strategic positions and cooperatively corrupt the collected information. With a large number of cloned nodes under command, the adversary may even gain control of the whole network. Furthermore, the node clone will exacerbate most of inside attacks against sensor networks. 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. 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.

II. LITERATURE REVIEW

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 sensor 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

- ✓ Among many physical attacks to sensor networks, the node clone is a serious and dangerous one.

Copyright to IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 2, Issue 7, July 2015

- ✓ Insufficient storage consumption performance in the existing system and low security level.

III. PROPOSED WORK

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 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.

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:

- ✓ 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.

IV. SYSTEM DESIGN

Systems design is the process or art of defining the architecture, components, modules, interfaces, and data for a system to satisfy specified requirements. One could see it as the application of systems theory to product development. There is some overlap and synergy with the disciplines of systems analysis, systems architecture and systems engineering.

System Architecture

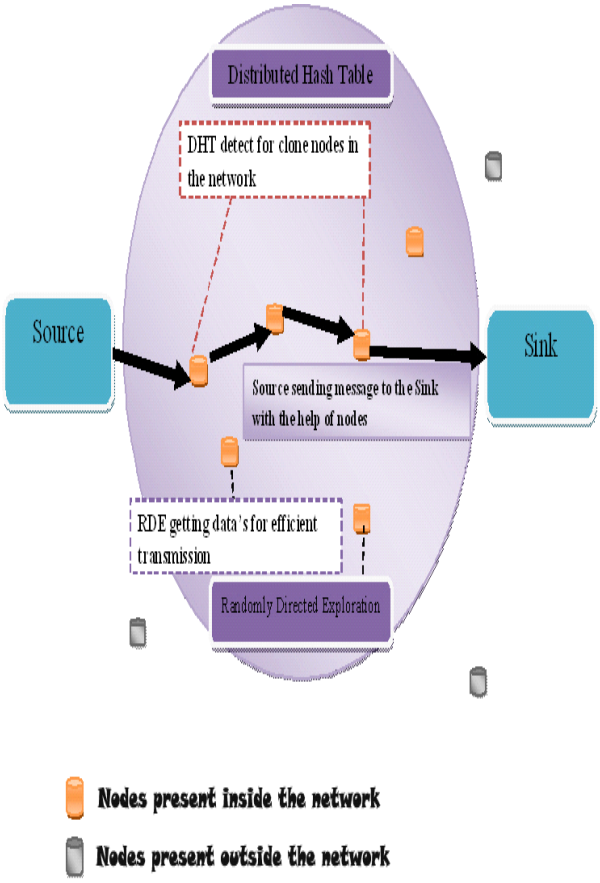

Fig.1. System Architecture

Block Diagram

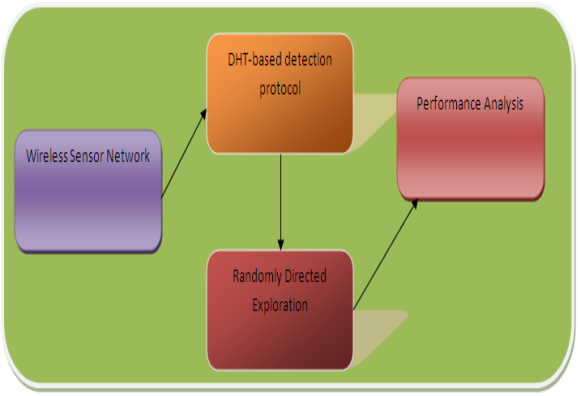

Fig.2. **Block Diagram**

Data Flow Diagram

- The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.
- The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.

Copyright to IARJSET
DOI 10.17148/IARJSET.2015.2719

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 2, Issue 7, July 2015

- DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.
- DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.

Dataflow Diagram

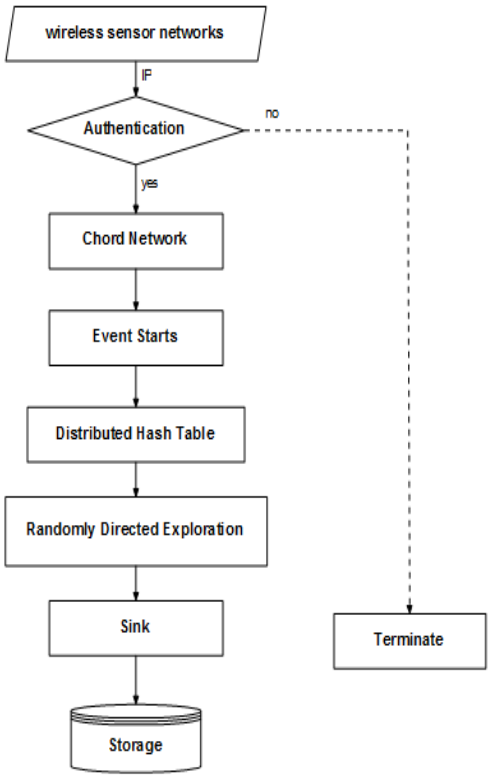

Fig.3. Dataflow Diagram

V. 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.

VI. FUTURE ENHANCEMENT

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 sensor nodes, which usually scatter in the surveillance area randomly, working without attendance. 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. 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.

ACKNOWLEDGEMENT

G. Sunil Kumar Author thanks to **M. NARESH BABU** Assistant Professor, Department of Computer Science & Engineering, Vaagdevi Institute of Tech & Science, Proddatur for his valuable guidance and chaperon. The real mentor and motivator of this project **U. SESHADRI** Assistant Professor, Department of Computer Science & Engineering, Vaagdevi Institute Of Tech & Science, Proddatur for giving us the opportunity to work with him and for all his efforts, patience and his encouragement, is gratefully acknowledged.

REFERENCES

[1] http://en.wikipedia.org/wiki/Wireless_sensor_network.
[2] Sohraby, K., Minoli, D., Znati, T. "Wireless sensor networks: technology, protocols, and applications", John Wiley and Sons, 2007 ISBN 978-0-471-74300-2, pp. 203–209
[3] http://en.wikipedia.org/wiki/Quality_of_service
[4] Leonard Franken. Quality of Service Management: A Model-Based Approach. PhD thesis, Centre for Telematics and Information Technology, 1996
[5] http://www.sciencedirect.com/science/article
[6] www.ra.ethz.ch/cdstore/www2005/docs/p1060.pdf

BIOGRAPHIES

I am **G. Sunil Kumar**, PG scholar. I had attended a handful number of conferences. From childhood onwards I am very interested to participate in extracurricular activities, that trait encouraged me to be a part in technical symposiums and journal publications. Despite an ordinary student my guide M. NARESH BABU Sir made me an extra ordinary student in my PG life, from bottom of my heart I thank **to M. NARESH BABU.**

I am **M. NARESH BABU**, Assistant Professor in Vaagdevi Institute of Tech & Science, Proddatur, Kadapa, India. I have been guiding technical students in various aspects in their Engineering life for the past four years. I motivated students especially in participating paper presentations, conferences including both national and international and journal publications.