Available online at: http://www.advancedscientificjournal.com
http://www.krishmapublication.com
IJMASRI, Vol. 1, issue 1, pp. 139-143, Apr. -2025
https://doi.org/10.53633/ijmasri

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY ADVANCED SCIENTIFIC RESEARCH AND INNOVATION (IJMASRI)

ISSN: 2582-9130 **IBI IMPACTFACTOR 1.5** **DOI: 10.53633/IJMASRI**

RESEARCH ARTICLE

ENERGY AND MEMORY EFFICIENT CLONE DETECTION IN WIRELESS SENSOR NETWORKS

Mrs Prabavathi[1] N Vennila S[2] and Sathya R[3]

[1]*PG & Research Department, Department of Computer Science, St.Ann's College of Arts and Science, Tindivanam.*
Email: prabatamil18@gmail.com

[2]*Principal & Head of the Department, PG & Research Department of Computer Science, St.Ann's College of Arts and Science Tindivanam*
Email: sathiyaat@gmail.com

[3]*Assistant Professor & Head, Department of Computer Science, St.Ann's College of Arts and Science Tindivanam.*
Email: moulikrishna19@gmail.com

Abstract

In this paper, we propose an energy-efficient location-aware clone detection protocol in densely deployed WSNs, which can guarantee successful clone attack detection and maintain satisfactory network lifetime. Specifically, we exploit the location information of sensors and randomly select witnesses located in a ring area to verify the legitimacy of sensors and to report detected clone attacks. The ring structure facilitates energy-efficient data forwarding along the path towards the witnesses and the sink. We theoretically prove that the proposed protocol can achieve 100 percent clone detection probability with trustful witnesses. We further extend the work by studying the clone detection performance with untrustful witnesses and show that the clone detection probability still approaches 98 percent when 10 percent of witnesses are compromised. Further, the necessary buffer storage of sensors in the majority of current clone detection protocols with random witness selection schemes is typically dependent on the node density, or O(n−−√),whereas in our suggested protocol, the required buffer storage of sensors is independent of n but a function of the hop length of the network radius h, or O(h). By efficiently dispersing the traffic load throughout the network, our suggested protocol can achieve a long network lifetime, as shown by extensive simulations.

Keywords: Sensors, Clone, Protocol

Introduction

Wireless sensors have been widely deployed for a variety of applications, ranging from environment monitoring to telemedicine and objects tracking, etc. For cost-effective sensor placement, sensors are usually not tamper-proof devices and are deployed in places without monitoring and protection, which makes them prone to different attacks. For example, a malicious user may compromise some sensors and acquire their private information.. Then, it can duplicate the sensors and deploy clones in a wireless sensor network (WSN) to launch a variety of attacks, which is referred to as the clone attack. As the duplicated sensors have the same information, e.g., code and cryptographic information, captured from legitimate sensors, they can easily participate in network operations and launch attacks.

Clone attacks have emerged as one of the most important security threats in WSNs because of the low cost of sensor deployment and replication. Therefore, ensuring the properoperation of WSNs requires the effective detection of clone attacks. Typically, a group of nodes known as witnesses are chosen to help verify the validity of the nodes in the network, enabling effective clone detection. During the witness selection process, witnesses are given access to the source node's sensitive information, such as their identity and location.

Any node in the network that wishes to communicate data first asks the witnesses to verify its validity; if the node is unable to do so, the witnesses will report a detected attack. Two conditions must be met via witness selection and authenticity verification in order to successfully detect clones: At least one witness must be able to correctly receive all of the verification messages for clone detection, and witnesses should be chosen at random.

In order to prevent malicious users from creating duplicate verification messages, the first requirement is to make it difficult for them to intercept the communication between the current source node and its witnesses. The ability of at least one witness to verify the identity of the sensor nodes in order to as certain whether or nota clone assault is occurring is the second prerequisite. It is crucial and difficult to meet these parameters in the design of clone detection protocols in order to provide a high clone detection probability, or the likelihood that clone assaults may be successfully detected.

Nevertheless, the majority of methods primarily concentrate on increasing the likelihood of clone identification without taking efficiency and energy balance in WSNs into account. Such methods may lead certain sensors to deplete their batteries as a result of their uneven energy use, and dead sensors may split the network, further impairing WSNs' ability to function normally.

It is crucial to balance the energy consumption of sensors distributed across various WSN areas in addition to minimizing the energy consumption of each node in order to extend the network lifetime, or the amount of time from the network's inception until the first instance of a sensor running out of energy. Another crucial aspect of sensors that significantly affects the design of clone detection algorithms is their limited memory or data buffer. In general, witnesses must document the private information of source nodes and validate the authenticity of sensors using the stored private information in order to ensure successful clone detection.

Sensors in high-density wireless sensor networks (WSNs) require a large buffer to record the information that is transmitted between them; hence, the required buffer size grows with the network node density. This is the case for the majority of current clone detection techniques.

The protocol can be used in general multi-hop WSNs that are densely deployed, where attackers could compromise and clone sensor nodes to initiate assaults. A draft of the work is shown. In order to obtain a high clone detection probability with random witness selection and maintain normal network operations with a satisfactory network lifetime of WSNs, we presented an energy-efficient ring-based clone detection (ERCD) protocol in that study. The two phases of the ERCD procedure are validity verification and witness selection.

In witness selection, a group of witnesses is chosen at random by the mapping function after receiving private information from the source node. Verification messages and the source node's private information are sent to its witnesses as part of the validity verification process. The message will be forwarded to its witness header for verification if any of the witnesses successfully receive it. The witness header compares the combined verification messages with the stored records after receiving the messages.

The clone attack is identified and a revocation procedure is initiated if several copies of the verification messages are received. Therefore, in order to conduct a thorough analysis of the ERCD protocol, we expand the analytical model by assessing the protocol's necessary data buffer and adding experimental findings to bolster our theoretical analysis. First, using reliable witnesses, we theoretically demonstrate that our suggested clone detection methodology may get probability

1. Taking into account the possibility of compromised witnesses, our simulation results show that, when employing the ERCD protocol, the clone detection probability can still be close to 98 percent inWSNswith10percent cloned nodes. Second, we determine the expression of total energy consumption and compare our protocol with other clone detection procedures in order to assess the performance of network longevity. We discover that by distributing the witnesses among WSNs—with the exception of non-witness rings, such as the nearby rings surrounding the sink, which shouldn't contain witnesses—the ERCD protocol can balance the energy consumption of sensors at various places. Next, using the function of energy usage, we determine the ideal number of non-witness rings.

Lastly, we use the ERCD protocol to extract the expression of the necessary data buffer and demonstrate the scalability of our suggested protocol by demonstrating that the necessary buffer storage depends solely on the ring size. With an appropriate data buffer capacity, our suggested ERCD protocol can achieve superior performance in terms of network lifetime and clone detection probability, according to extensive simulation results.

Literature Review

Using Randomized Multipath Routing to Gather Secure Data. There are several uses for wireless sensor networks, or WSNs. Security issues thus take on greater significance. In a static WSN with a single base station, we study the issue of reducing the packet delivery failure rate in the presence of selective forwarding and modification assaults without the need for costly encryption / decryption algorithms. We offer a brand-new heuristic solution to this issue. Design concepts and enhancements to energy-aware routing algorithms for wireless sensor networks based on cost functions

In wireless sensor networks, cost function-based routing has been extensively researched to increase energy efficiency and network lifetime. However, current methods have a number of drawbacks because of the problem's complexity. The fundamental factors, design concepts, and assessment techniques for cost function-based routing algorithms are examined in this work. This work proposes two energy-aware cost-based routing algorithms: Double Cost Function based Route (DCFR) and Exponential and Sine Cost Function based Route (ESCFR). Small variations in the nodal remaining energy can be translated into significant variations in the function value for ESCFR thanks to its cost function.

Analysis

In the fields of information systems, software engineering, and systems engineering, the process of developing or modifying systems, as well as the models and techniques employed in the process, is known as the Systems Development Life Cycle (SDLC) or Software Development Life Cycle. Numerous software development approaches in software engineering are based on the SDLC idea. These approaches serve as the foundation for organizing and managing the software development process and the establishment of an information system.

Existing System

The majority of methods primarily concentrate on increasing the likelihood of clone

identification without taking efficiency and energy balance in WSNs into account. Such methods may lead certain sensors to deplete their batteries as a result of their uneven energy use, and dead sensors may split the network, further impairing WSNs' ability to function normally. It is crucial to balance the energy consumption of sensors distributed across various WSN areas in addition to minimizing the energy consumption of each node in order to extend the network lifetime, or the amount of time from the network's inception until the first instance of a sensor running out of energy.

Present System

In this research, we present a distributed clone detection protocol with a random witness selection mechanism in WSNs that is energy- and memory-efficient, taking into account not only the clone detection probability but also energy consumption and memory storage. Our approach can be used in general densely distributed multi-hop WSNs, where attackers could clone and compromise sensor nodes to initiate assaults. In earlier research, we suggested an energy-efficient ring- based clone detection (ERCD) protocol that ensures normal network operations and a good network lifetime of WSNs while achieving a high clone detection rate with random witness selection.

Software Requirement Specification

A comprehensive description of the behaviour of a system that has to be constructed is called a Software Requirements Specification (SRS). It contains a collection of use cases that outline every interaction users will have with the program. The SRS includes non-functional requirements in addition to use cases. Requirements that place limitations on the design or implementation are known as non-functional requirements. Examples of these include design restrictions, performance engineering requirements, and quality standards.

IMPLEMENTATION

The Frame class, defined in the java.awt package, will be extended in the first method to create a frame. The following software show to create a frame. The public class FrameDemo1 extends Frame {FrameDemo1(); importjava.awt.*;

{ public static void main(String[] args) {new Frame Demo1 ();}} {set Title ("Label Frame"); set Visible (true); set Size (500,500);} Three techniques are employed in the program mentioned above: set Title: We'll use this technique to set the frame's title. The title name is String, which is passed in as an argument. Set Visible: This is how we will make our frame visible. Boolean values are used as arguments in this method. The window will be visible if we are passing true; otherwise, it won't be Set Size: This method will be used to set the window's size. The frame's width and height are the first and second arguments, respectively.

Method 2: To create a frame window, we will create an instance of the Frame class in this method. Method2 is demonstrated by the following program:import java.awt.*;public class FrameDemo2

{String [] args{Public staticvoid main

{Frame f = new Frame (); f.set Size (500,500); f.set Visible(true); f.setTitle ("My first frame");} }

CONCLUSION

We present a distributed, energy-efficient clone detection approach with random witness selection in this study. In particular, the witness selection and legitimacy verification phases are part of the ERCD protocol that we have suggested. Since each sensor node's witnesses are dispersed in a ring structure, which makes it simple to accomplish by sending a verification message, our protocol can detect clones with about a one percent chance, as shown by both our theoretical analysis and simulation results.

Additionally, with an appropriate data buffer storage capacity, our protocol can improve network lifetime and overall energy usage. In order to reduce the energy consumption and memory storage of the sensor nodes surrounding the sink node and increase the network lifetime, we utilize the location information to distribute the traffic load across WSNs.

References

1. InProc.IEEEINFOCOM,Apr.14-19,2013,pp.2436 2444, Z. Zheng, A. Liu, L.X. Cai, Z. Chen, and X .Shen published "ERCD: An energy-efficient clone detection protocol in WSNs."
2. R.Lu,X. Li,X. "GRS: The green, reliability, and security of emerging machine to machine communications," IEEE Commun. Mag., vol.49, no.4, pp.28–35,April2011,
3. "Wireless sensor networks: A survey," Comput. Netw., vol. 38, no. 4, pp. 393–422, March 2002, F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci
4. "Design principles and improvement of cost function based energy aware routing algorithms for wireless sensor networks," byLiu, J. Ren, X. Li, Z. Chen, and X. Shen, Comput. Netw., vol. 56,no.7,pp.1951–1967,May2012.
5. T. Shu, M. Krunz, and S. Liu, "Using randomized dispersive routes to secure data collection in wireless sensor networks," IEEETrans. Mobile Comput., vol. 9, no. 7, pp. 941–954, July 2010.
6. "A randomized countermeasure against parasitic adversaries in wireless sensor networks,"IEEEJ.Sel.AreasCommun.,vol.28, no. 7, pp. 1036–1045, September 2010, P. Papadimitratos, J. Luo, and J. P. Hubaux.

******