International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Energy and Memory Efficient Clone Detection in Wireless Sensor Networks

Dr.Mohammed Abdul Bari,
Associate Professor of CSE Department,
Mohammed Shabbir Ali, Siddiqui Akbar Quadri, Ahmed Khan,
UG Students
IT Department
ISL Engineering College, Telengana.

ABSTRACT:

In this research, we present an energy-efficient, location-aware clone detection strategy for densely distributed WSNs that can identify clone assaults and maintain the network alive for a long period. In specifically, we utilize the position information of sensors and randomly pick witnesses in a ring region to make sure that sensors are authentic and to report clone assaults that we uncover. The ring topology makes it simpler to deliver data along the route to the witnesses and the sink in a manner that requires less energy. Theoretically, we demonstrate that the suggested technique can have a 100 percent probability of identifying a clone with trustworthy witnesses. We contribute to the study by looking at how effectively clones can be discovered when witnesses don't speak the truth. We demonstrate that even when 10 percent of witnesses lie, the likelihood of detecting a clone is still close to 98 percent. Also, in most existing clone detection protocols with a random witness selection scheme, the required buffer storage of sensors depends on the number of nodes, or O(n), while in our proposed protocol, the required buffer storage of sensors depends on the hop length of the network radius, or O(h) (h) (h). Extensive simulations demonstrate that our suggested protocol may help a network survive longer by dispersing the traffic load throughout the network in an efficient manner.

Introduction:

From environmental monitoring to telemedicine to item tracking, wireless sensors have seen extensive usage. Sensors are sometimes not built to be tamper-proof and are placed in areas where they won't be observed or safeguarded in order to save money on sensor installation. As a result, they are susceptible to a wide range of assaults. A malicious person, for example, may seize control of sensors and steal sensitive information. Afterwards, it may replicate the sensors in a wireless sensor network (WSN) and use them to carry out a wide range of cyberattacks. The "clone attract" is the term for this effect. It is simple for the duplicate sensors to participate in network activities and launch attacks since they contain the same code and cryptographic information as the original sensors. Because it is so easy to build a copy of a sensor and install it in place, clone attacks have become one of the most serious security issues in WSNs. As a result, it is critical for WSNs to function properly so that clone attacks may be halted. In order to find clones rapidly, a set of nodes called "witnesses" is usually selected to assist validate that the other nodes in the network are genuine. The source node's private information, such as its name and location, is shared with the witnesses at this step. In order to communicate data, a node in the network first asks the witnesses for their approval. Nodes that fail the certification process will be reported as a security breach by witnesses.

Existing System:

One of the most essential aspects of clone detection procedures is the sensor's limited memory or data buffer. For clone detection to succeed, witnesses must collect the private information of source nodes and utilize this information to ensure that sensors are genuine.. In most current clone detection techniques, the buffer storage capacity is determined by the number of network nodes. A high-density WSN requires a large buffer to hold the information shared by sensors, hence the buffer size rises as the number of nodes in the network increases. Because of this, current protocols are not ideal for WSNs that are put up in a wide variety of locations. For WSNs that are put up in a wide variety of locations, current procedures aren't as

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

good as they might be. For sensor networks with limited energy and memory, several current approaches can enhance clone detection, but they need a lot of energy and memory, which may not work.

Literature survey:

In a broad variety of applications, wireless sensor networks (WSNs) are becoming more significant, from monitoring hazardous surroundings to providing medical telemedicine. Sensor nodes are prone to clone attacks because to their hardware and cost limits, making it difficult to design and set up a WSN that utilizes energy effectively. In this study, we offer a clone detection technique that takes into account the location of the clone attack in order to ensure that it is detected while causing as little damage as possible to the network. The position information of sensors is used in particular to ensure that sensors' privacy is preserved and to detect clone assaults. In addition, we randomly choose witness nodes in a ring region. The ring construction saves energy while making it simpler to send data to the witnesses and sink. Because the traffic load is distributed over the network, it lasts far longer than with a single point of failure, If the witnesses can be believed, theoretical analyses and simulations reveal that the suggested approach has a near-perfect likelihood of discovering clones. When some of the witnesses can't be believed, we look at how well clones can be discovered. When just 10% of the witnesses can be believed, we still have a nearly 98% chance of detecting clones. In addition, our suggested protocol has the potential to significantly extend the life of the network when compared to the present one.

The green, reliability, and security of emerging machine to machine communications

It's when a big number of smart robots work together without human involvement to exchange information and make choices. A broad variety of real-time monitoring applications, including remote healthcare, smart homes, environmental monitoring, and industrial automation, have benefited greatly from M2M communications. This is due to the fact that it has the ability to accommodate a large number of common features while also reducing costs. Despite this, the development of M2M communications still relies on how effectively we understand and deal with the issues we presently face, such as green energy efficiency, dependability and security (GRS). Without a guarantee of GRS, M2M communications will not be generally acknowledged as a potential mode of communication. M2M communications are examined in this article in light of prospective GRS concerns. To do this, we're working to create a more energy-efficient and dependable M2M communication environment. The M2M communications architecture is first formalized to encompass the M2M, network, and application domains, and the GRS requirements are then defined in a systematic manner based on that framework. In the next section, we discuss certain GRS-enablement strategies, such as activity scheduling, redundancy, and cooperative security mechanisms. Using these techniques, M2M communication apps might be developed and deployed more quickly.

Disadvantage:

Here's a sneak peek at a work in progress. This study suggested an energy-efficient ring-based clone detection (ERCD) protocol to achieve high clone detection probability with random witness selection, while maintaining normal network operations and a suitable network lifespan for WSNs.

There are two phases to the ERCD protocol: selecting witnesses and verifying their claims of identity. The source node transmits its private information to a group of witnesses during witness selection. These witnesses are selected at random by the mapping function. The source node's private information is provided to its witnesses together with a verification message in the validity check.

There are normally sinks or witnesses located in the centre of each zone, where sensors' private information is stored, in centralized protocols. They may check for a clone attack by comparing the source node's private information with its previously stored records when the sink or witnesses get this information.

Proposed System:

Sending data to witnesses and the sink without wasting too much energy is made possible by the rings. A clone may be detected using the suggested methodology with the help of trustworthy witnesses, according to our theoretical calculations. When some of the witnesses can't be believed, we

look at how well clones can be discovered. When just 10% of the witnesses can be believed, we still have a nearly 98% chance of detecting clones.

Let us start by showing the probability of one that may be obtained by using our suggested clone detection method when it is based on reliable witnesses. We've shown in our simulations that the ERCD protocol can discover clones in WSNs with 10% copied nodes even if the witnesses are tampered with.

As a second step, we calculate how much energy the network consumes throughout its lifespan and compare our protocol to other clone detection algorithms. By placing witnesses in all WSNs except the non-witness rings, which are those adjacent to the sink and should not have witnesses, we discovered that the ERCD protocol can ensure that sensors in various locations utilize the same amount of energy.

Advantage:

There has to be a balance between the amount of energy used and the amount of data stored in buffers when employing random witness selection methods for clone detection. Others, like Parallel Multiple Probabilistic Cells (P-MPC), proposed a strategy that attempted to combine the advantages of both random and deterministic methods of identifying clones in a distributed manner.

The mapping function is used to determine a deterministic area for the source node in this sort of witness selection technique. Random witnesses for the source node are then selected from sensors in this area. Because each sensor has a random set of witnesses, this adds a significant amount of overhead and temporal complexity.

This is due to the fact that we distribute traffic between WSNs based on geographic information. There is less data to store and less energy used by sensors located near the sink node, which helps the network survive longer. We'll think about how individuals move about in various network settings in the future.

The discipline of computer science that encompasses data mining is known as data mining. Artificial Intelligence, machine learning, statistics, and database systems are used to detect patterns in enormous volumes of data (referred to as "big data"). The primary purpose of the data mining process is to extract information from a collection of data and transform it into a structure that is simple to comprehend and can be utilized in a variety of different ways. " Database and data administration, pre-processing, model considerations (interestingness metrics), complexity considerations, post-processing of identified structures (viz., visualization), and online updating are all part of this process. Data mining is a part of the "knowledge discovery in databases" (KDD) process. Data mining is the practice of analyzing massive volumes of data in order to discover previously unknown patterns. Cluster analysis, anomaly detection, and dependencies are all examples of these patterns (association rule mining). Database approaches like spatial indices are often used to do this. In this way, the patterns may be considered as a kind of summary for the data that was entered into the system They may be used in a variety of ways, such as in the development of machine learning algorithms and predictive analytics. As an example, a data mining process may identify numerous groupings in the data, which a decision support system could subsequently utilize to create more precise predictions. In the KDD process, data collection, data preparation, and reporting the findings are not part of the data mining stage, yet they are.

According to the definitions of data mining, the term "dredging," "fishing," and "snooping" all mean the same thing: extracting data from a wider population to draw judgments about the validity of any patterns identified. This strategy may be used to generate new hypotheses that can be evaluated against bigger data sets.

The term "Big Data" refers to the collection and analysis of enormous amounts of data from a wide variety of sources. All branches of research and engineering, including physics, biology, and biomedicine, are seeing rapid growth in the amount of Big Data being generated. Data storage, network connectivity, and data collection are all developing at a rapid pace. This article provides a HACE theorem, which characterizes the Big Data revolution and proposes a Big Data processing paradigm, from a data mining perspective. Based on what users desire, this model gathers information sources, mines and analyzes data, models user interests, and considers security and privacy. We examine the drawbacks of the Big Data revolution and the data-driven paradigm.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Technique:

There are three main considerations in this paper: the probability of discovering an identical copy, the network's lifespan, and how much data has to be held in the buffer. The goal is to create a distributed clone detection technique with random witness selection. Initially, just a few nodes are taken over by nefarious individuals.

As part of the clone detection methodology, we want to increase the likelihood that a cloned node will be discovered. To ensure the safety of WSNs, this procedure is followed. At the same time, we must ensure that the data gathering and clone detection process are not hindered by a lack of energy or buffer storage. Hence, it is important to avoid having a short network lifespan (the period between the start of operation and the first outage).

Methodology:

Wireless sensor nodes in WSNs are often powered by batteries, therefore it is critical to track how much energy they use and ensure that node failure does not disrupt the network.

For this reason, the ERCD protocol's lifespan is defined as how long it takes for a network node to cease functioning. Because the power needed for receiving is so minimal, we solely consider the power utilized for transmission. ERCD employs ring structures to generate witness sets, so sensor nodes in the same ring do identical tasks.

A witness's capacity to receive the verification message from the source node is typically what determines the likelihood of a successful clone detection in a distributed protocol with random witness selection. So, the ERCD protocol's clone detection probability is the likelihood that the verification message can be transmitted from the source node to its witnesses, as explained above.

HUMAN-MACHINE INTERFACE

As a user/operator, you will find detailed information on the system and its subsystems' inputs and outputs here. To better display the operator's input and output designs, this section may be customized to include any additional information. These parts may need to be repeated at the subsystem and design module levels, depending on the nature of the project. More information may be contributed to the subsections if the lists provided do not adequately define the project's inputs and outputs.

Inputs

Information that the operator may provide to the system is described in this section. An additional mapping to Section 1.2.1, System Overview, should also be included. For example, data entry displays, optical character readers, bar code scanners, and so on. Data structures from Section 3 of this manual (File and Database Design) may be utilized if they make sense as input record types. Use the data dictionary or provide definitions of data items.

All graphical user interfaces (GUTs) or displays for inputting data should be laid out in detail (for example, windows). Provide a visual representation of each user interface. Use the data dictionary or define each data element for each screen or GUI.

Specify edit criteria for data components, including particular values, ranges of values, mandatory/optional, alphanumeric values, and length. The controls for inputting data should also be taken care of such that modifications cannot be bypassed.

Outputs

Using the user/point operator's perspective, this section describes how the system's output is developed. As a result, Section 1.2.1's high-level data flows are shown in Section 1.2.2's output. Results of queries and other operations are some examples of the many types of output generated by the system. It is possible to make use of Part 3's explanation of the output files in this section. As a last resort, the following should be included:

Identification of report and data display screen codes and names The report and the screen content (provide a graphic representation of each layout and define all data elements associated with the layout orreference the data dictionary)

A description of the output's purpose, including who the primary consumers are. Distribution criteria should be specified (include frequency for periodic reports) Information about access and security limitations.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

SYSTEM TESTING

In order to discover errors, testing is necessary. Testing is the practice of searching for any and all flaws or weaknesses in a piece of work that may exist. Using it, you can see how effectively individual parts, subassemblies, and assemblies operate together. Software testing ensures that the product satisfies its specifications and user expectations and does not fail in an unacceptable manner. There are a wide variety of tests available. There is a specific purpose for each test type.

System Test

During system testing, the testers verify that the whole integrated software system meets the standards they've set forth for it. To guarantee that the results can be predicted in advance, it performs a series of tests on the configuration. The configuration-oriented integration test is an example of a system test. System testing is guided by a process description and flow, with an emphasis on linkages and integration points that have previously been defined in the process. Testing in a controlled setting without the use of equipment is known as "White Box Testing."

White box testing is when a software tester is familiar with the program's internal workings, structure, and language, or at the very least, the product's aim. The endgame is obvious. Using this method, it is possible to test sites that are not accessible from a black box level.

Black Box Testing

In Black Box Testing, the testers assume no knowledge of the software module's internal workings, structure, or language. Like most other kinds of tests, black box testing requires a source document, such as a specification or requirements document, to be used as the starting point. It is called "black box testing" when the software being tested is treated as if it were an entirely other piece of software. It's not feasible to see inside of it. The test doesn't examine how the software works, but rather provides inputs and responds to the outputs.

Unit Testing:

Most of the time, coding and unit testing are carried out in tandem throughout the software development lifecycle, although this is not always the case. Field testing will be done by hand, and functional tests will be set up in great detail.

Test objectives

There must be no errors in any of the data entered.

• Pages may only be accessed by clicking on the link that has been provided. An entry screen, messages and answers should not be delayed.

Conclusion:

The clone detection system proposed in this work is distributed and uses a random selection of witnesses. If you'd want to know more about how we came up with our suggested ERCD protocol, here's a breakdown:

A clone assault can nearly always be detected by our procedure, as proved by both our theoretical analysis and simulations. Due to the fact that each sensor node's witnesses are widely dispersed, it is simple to transmit a verification message.

Our approach may extend the network's lifespan and reduce its energy consumption by using a big enough data buffer. This is due to the fact that we distribute traffic between WSNs based on geographic information. There is less data to store and less energy used by sensors located near the sink node, which helps the network survive longer. We'll think about how individuals move about in various network settings in the future.

In the future:

For the proposed ERCD protocol, we look at duty cycles and the average delay and routing success rate, which is the rate of successful routing throughout all transmission rounds with varied duty cycles.

We envision a WSN with a transmission range of 50 meters for each sensor node in a 500m500m region. Sensor nodes in the ERCD protocol may transmit messages to other sensors that are awakened.

It will keep onto the message until one of the sensors surrounding it wakes up or the delay period runs out, whichever comes first. The round of clone detection routing fails if any node's communication takes longer than 1 second.

This is because, unlike in other protocols, the number of witnesses in LSM relies on the number of nodes. Storage requirements may be reduced by increasing the number of nodes or increasing the density of the nodes.

Reference:

[1] Z. Zheng, A. Liu, L. X. Cai, Z. Chen, and X. Shen, "ERCD: An energy-efficient clone detection protocol in wsns," in Proc. IEEE INFOCOM, Turin, IT, Apr. 14-19 2013, pp. 2436–2444.

[2] R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, "GRS: The green, reliability, and security of emerging machine to machine communications," IEEE Communications Magazine, vol. 49, no. 4, pp. 28–35, Apr. 2011.

[3] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," Computer Networks, vol. 38, no. 4, pp. 393–422, Mar. 2002.

[4] A. Liu, J. Ren, X. Li, Z. Chen, and X. Shen, "Design principles and improvement of cost function based energy aware routing algorithms for wireless sensor networks," Computer Networks, vol. 56, no. 7, pp. 1951–1967, May. 2012.

[5] T. Shu, M. Krunz, and S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," IEEE Transactions on Mobile Computing, vol. 9, no. 7, pp. 941–954, Jul. 2010.

[6] P. Papadimitratos, J. Luo, and J. P. Hubaux, "A randomized countermeasure against parasitic adversaries in wireless sensor networks," IEEE Journal on Selected Areas in Communications, vol. 28, no. 7, pp. 1036–1045, Sep. 2010.

[7] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in VANETs," IEEE Transactions on Vehicular Technology, vol. 61, no. 1, pp. 86–96, Jan. 2012.

[8] Z. M. Fadlullah, M. Fouda, N. Kato, X. Shen, and Y. Nozaki, "An early warning system against malicious activities for smart grid communications," IEEE Network, vol. 25, no. 5, pp. 50–55, May. 2011.

[9] R. Lu, X. Lin, X. Liang, and X. Shen, "A dynamic privacy-preserving key management scheme for location based services in VANETs," IEEE Transactions on Intelligent Transportation Systems, vol. 13, no. 1, pp. 127–139, Jan. 2012.

[10] M. Conti, R. D. Pietro, L. Mancini, and A. Mei, "Distributed detection of clone attacks in wireless sensor networks," IEEE Transactions on Dependable and Secure Computing, vol. 8, no. 5, pp. 685–698, Sep.- Oct. 2011.