International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET

Wireless Sensor Networks with Efficient Clone Detection in Terms of Energy and Memory

Sana Afia[*1], **Dr. B. Sasi Kumar**[*2]

[*1] M.Tech Student- CSE, Department of Computer Science Engineering, Dr. V. R. K. Women's College of Engineering & Technology, Hyderabad, Telangana, India

[*2] Principal & Professor, Department of Computer Science Engineering, Dr. V. R. K. Women's College of Engineering & Technology, Hyderabad, Telangana, India

Article Info
Volume 9, Issue 5
Page Number : 240-247

Publication Issue :
September-October-2022

Article History
Accepted : 10 Oct 2022
Published: 30 Oct 2022

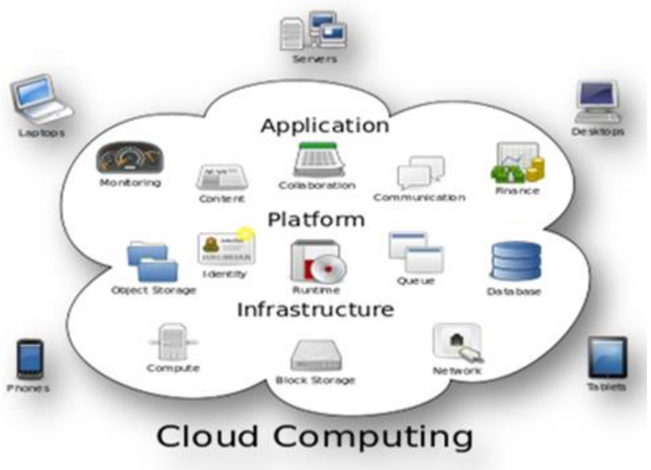
ABSTRACT

We propose an energy-efficient location-aware clone detection protocol for densely deployed WSNs to ensure successful clone attack detection and satisfactory network lifetime. Using the sensors' geolocation data, we randomly select witnesses within a ring area to attest to the sensors' legitimacy and report any clone attacks they may have uncovered. The witnesses and the sink along the path can receive data with minimal power consumption thanks to the ring topology. For the first time, we theoretically show that the proposed protocol can achieve a clone detection probability of one hundred percent with trustworthy witnesses. In this expanded work, we examine clone detection performance with untrustful witnesses and find that, even with 10% of witnesses being compromised, the clone detection probability is still very close to 99%. The proposed protocol also requires buffer storage of sensors that depends not on the number of sensors, n, but on the network's radius, h, i.e. Oh, whereas the required buffer storage of sensors is typically dependent on the node density in existing clone detection protocols with random witness selection scheme. Extensive simulations show that our proposed protocol can ensure a long network lifetime by evenly distributing the traffic load across the network.

Keywords : Wireless Sensor Networks, Clone Detection Protocol, Energy Efficiency, And Network Lifetime

I. INTRODUCTION

Cloud computing (equipment and software) is used and shared remotely over a network in what is known as "the cloud" (usually the Internet). In structure graphs, a cloud-shaped picture is commonly used to represent the complex information it contains, hence the name. Through distributed processing, a client's information, code, and estimation can be shared amongst multiple, geographically dispersed organizations. System hardware and software for appropriate processing are available online from supervised pariah groups. Modern programming languages and server PC networks are made possible by these establishments.



Structure of cloud computing

Explaining the Workings of Cloud Computing

Traditional supercomputing, or peak execution handling power, is typically reserved for use by the military and assessment agencies. The purpose of distributed registration is to put this type of processing power to use in client-centric applications, such as financial portfolios, the transmission of updated information, the provision of data limits, and the management of massive, visually impressive PC games. Distributed processing makes use of networks of very large groups of servers, which typically run low-cost client PC development and have some connection to dispersing data-handling tasks. Common IT architectures feature massive aggregations of interconnected systems. Virtualization methods are commonly used to increase the efficiency of distributed computing. Characteristics and Service Types: With the NIST's definitions in mind, here are some of the most remarkable aspects of widely disseminated numbers:

- Self-organization on demand: customer can set their limits for things like server time and association storage as needed, without needing to coordinate with each specialist facility individually.
- Capabilities are accessible over the network and can be used by a variety of client types thanks to standardized frameworks (e.g., cells, PCs, and PDAs).
- Resource pooling: In a multi-tenant model, the provider shares its enlisting resources among its many clients, allocating and reallocating its physical and digital assets to each client by their needs. Since the client generally has no control or data over the specific region of the provided resources at this point, there is a sense of region opportunity and the client may have the option to decide region at a higher level of reflection (e.g., country, state, or server ranch). Resource situations consist of constraints, management, memory, data transmission over networks, and virtual machines.
- Rapid adaptability: Capabilities can be provisioned quickly and skillfully, occasionally normally, to rapidly scale out, and immediately conveyed to rapidly scale in. Often, the client has the impression that they can purchase an unlimited amount of provisioning at any time.
- A metering limit appropriate to the type of business is typically used by cloud architectures to manage and expand resource utilization (e.g., limit, dealing with, information transmission, and dynamic client accounts). Both the user and the resource provider can benefit from due, controlled, and definitive resource use.

On-demand self-service
Ubiquitous network access
Location transparent resource pooling
Rapid elasticity
Measured service with pay per use

Characteristics of cloud computing

II. RELATED WORK

2.1 Protocol for detecting clones in wireless sensor networks that uses minimal power (ERCD)

Z. Zheng, A. Liu, L. X. Cai, Z. Chen, and X. Shen are the authors here.

As their capabilities continue to improve, wireless sensor networks (WSNs) are finding use in a growing number of fields, from the study of dangerous environments to the delivery of medical care remotely. However, due to hardware and cost limitations, sensors are vulnerable to clone attacks, which presents significant obstacles to developing and deploying an energy-efficient WSN. In this paper, we propose a location-aware clone detection protocol that can reliably identify clone attacks while minimizing their impact on the longevity of the network. To confirm sensor privacy and identify clone attacks, we utilize sensor location data and randomly select witness nodes in a ring area. Traffic load is spread out across the network, increasing network lifetime, and the ring structure allows for energy-efficient data forwarding along the path to the witnesses and the sink. Analyses and simulations show that the proposed protocol can nearly achieve a perfect clone detection probability with reliable witnesses. We further extend the work by investigating the performance of clone detection with untrustworthy witnesses, and we find that even when 10% of witnesses are compromised, the clone detection probability is still close to 98%. Moreover, in comparison to the current method, our proposed protocol can greatly increase the network's lifetime.

2. Sustainability, dependability, and safety in the next generation of M2M communications are the focus of Section 2.2 GRS.

R. Lu, X. Li, X. Liang, X. Shen, and X. Lin are the authors.

Communication between machines is characterized by a large number of autonomous machines exchanging data and reaching collective conclusions without the involvement of a human hand. M2M communications have become a game-changer for many real-time monitoring applications like remote e-healthcare, smart homes, environmental monitoring, and industrial automation because of their potential to support a large number of ubiquitous characteristics and achieve better cost efficiency. Nonetheless, the success of M2M communications depends on overcoming the current obstacles of green energy consumption, unreliable connections, and insecure data (GRS). No serious adoption of M2M communications as a promising communication paradigm can occur without GRS guarantees. This article's goal is to promote an energy-efficient, reliable, and secure M2M communications environment by examining the emerging field from the perspective of potential GRS issues. To be more precise, we first formally define GRS requirements by incorporating three domains into the M2M communications architecture: the M2M domain, the network domain, and the application domain. We then investigate activity scheduling, redundancy utilization, and cooperative security mechanisms as several GRS enabling techniques. These methods show potential for speeding up the creation and rollout of M2M communications software.

3 A review of wireless sensor networks

W. Su, Y. Sankarasubramaniam, E. Cayirci, and I. F. Akyildiz are the authors.

Applications such as remote environmental monitoring and target tracking are crucial uses for a wireless sensor network (WSN). This has been made possible by the development in recent years of increasingly affordable miniaturized and computationally capable sensors. These sensors can form a network by talking to one another through their built-in wireless interfaces. Environment, application design goals, cost, hardware, and system constraints are just some of the factors that must be taken into account when planning a WSN's architecture.

We divide the issues into three groups:

(1) The core infrastructure and OS,

(2) The communication protocol stack, and

(3) The network infrastructure and its deployment

And maintenance. We summarise the most significant progress made in these three areas and describe forthcoming difficulties.

4. Cost-function-based energy-aware routing algorithms for wireless sensor networks: design principles and enhancements

PUBLISHER(S): A. Liu, J. Ren, X. Li, Z. Chen, and X. Shen

To increase the network's efficiency with energy and to lengthen its lifespan, cost-function-based problem's complexity means that the current approaches all have their drawbacks. This paper examines the fundamentals, design principles, and evaluation techniques of cost-function-based routing algorithms. This paper proposes two cost-based routing algorithms that are also energy-aware: the Exponential and Sine Cost Function based Route (CFR) and the Double Cost Function based Route (DCFR). ESCFR's cost function can translate incremental shifts in nodal remaining energy to sizable shifts in overall function value. DCFR's cost function considers both the total energy used and the amount of energy left in each node, leading to a more efficient and equitable distribution of power. Analysis of the effectiveness of the cost function architecture is performed. Extensive simulations show the proposed algorithms outperform their rivals by a wide margin.

5 Using dispersed random paths for secure data collection in wireless sensor networks

T. Shu, M. Krunz, and S. Liu are the authors.

Key attacks in wireless sensor networks include compromised nodes and denial of service (WSNs). In this paper, we explore data delivery mechanisms that have a good chance of avoiding the black holes created by these attacks.

As a result of their deterministic nature, multipath routing approaches are susceptible to such attacks. Therefore, all data transmitted over these routes are open to attack once the adversary obtains the routing algorithm and can compute the same routes as the source. In this paper, we create a system to generate multipath routes at random. When implemented, our plans call for different packet "shares" to take different paths at different times. Therefore, the adversary cannot determine the paths taken by each packet even if the routing algorithm is compromised. The routes generated are not only completely random but also highly dispersed and energy efficient, making them more than capable of avoiding black holes. We perform an analytical study on the safety and efficiency of the proposed schemes. In addition, we formulate an optimization problem to reduce overall power usage while maintaining specified levels of safety. In-depth simulations are run to ensure the accuracy of our mechanisms.

III. SYSTEM ANALYSIS

3.1 Existing System

A group of nodes (witnesses) is typically chosen to attest to the network's nodes' authenticity in order to facilitate efficient clone detection. During the witness selection phase, the source node's identity and location are revealed to the witnesses. If a network node fails a certification check, the witnesses will report an attack. For clone detection to be successful, two criteria should be met in the selection and verification of witnesses:

1) It's necessary to choose witnesses at random;

2) At least one of the witnesses can receive the verification message(s) for detecting clones.

3) Threatening the efficient operation of WSNs are issues such as the uneven energy consumption of protocols like Randomized Efficient and Distributed (RED) and Line-Select Multicast (LSM), and the possibility of network partition brought on by dead sensors. Threatening the efficient operation of WSNs are issues such as the uneven energy consumption of protocols like Randomized Efficient and Distributed (RED) and Line-Select Multicast (LSM), and the

possibility of network partition brought on by dead sensors.

3.2 THE FLAWS IN THE CURRENT SYSTEM:

- Existing infrastructure does not guarantee that at least one witness can verify sensor node identities in the event of a clone attack; our goal, therefore, is to make it hard for malicious users to eavesdrop on the communication between the current source node and its witnesses.
- These requirements are critical but challenging to meet in clone detection protocol design, as they do not guarantee a high clone detection probability (the likelihood that clone attacks will be detected).
- When designing clone detection protocols for sensor networks, it is important to consider the energy and memory efficiency of sensors as well as to establish criteria that will lead to high performance in terms of clone detection probability.
- When a sensor's battery life starts to get low, it's important to make sure that sensors across the network are using their power efficiently and cooperatively.

3.3 PROPOSED SYSTEM

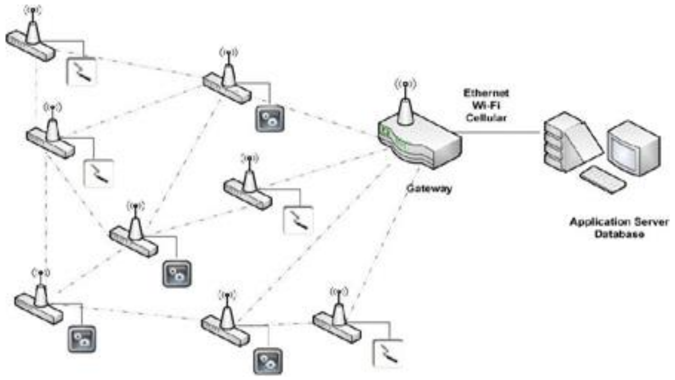
- For WSNs, we consider energy efficiency and memory needs alongside the clone detection probability as we design a distributed clone detection protocol with a random witness selection scheme.
- Our protocol can be used in networks with many nodes, such as multi-hop WSNs, and in which sensor nodes may be compromised or cloned by attackers.
- To further our analytic model, we evaluate the data buffer needs of the ERCD protocol and supplement our theoretical analysis with experimental results. The Powerful Method for Identifying Clone Rings.
- We find that the ERCD protocol can balance the energy consumption of sensors in different locations by spreading the witnesses across WSNs, with the exception of the non-witness rings, i.e. the adjacent rings around the sink, which should not have witnesses.
- Then, we use the energy budget to find the sweet spot for the number of rings that don't count as witnesses.
- Finally, we demonstrate the scalability of our proposed protocol by demonstrating that the required buffer size depends only on the size of the ring, an expression we derive using the ERCD protocol.

3.4 BENEFITS OF THE INTENDED SYSTEM:

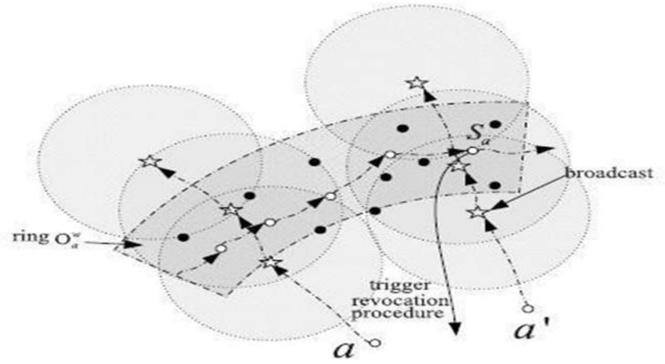
- The efficiency of the ERCD protocol is evaluated by examining its ability to detect clones, energy consumption, network lifetime, and buffer capacity.
- Our proposed ERCD protocol outperforms state-of-the-art solutions in terms of clone detection probability and network lifetime while keeping data throughput under control, as shown by extensive simulation results. This study demonstrates that even with unreliable witnesses, the probability of detecting a clone can approach 100%.
- The ERCD protocol reduces traffic of witness selection and legitimacy verification for sensors close to the sink, which helps to even out the energy consumption of data collection.

IV. SYSTEM DESIGN

4.1 SYSTEM ARCHITECTURE



BLOCK DIAGRAM



MODULES

- Module for System Construction
- Protocol for Early Reproductive and Child Determination
- Clone Detection Likelihood
- Concerns about longevity and energy use in networks

Module for Building Systems

- To test and implement our proposed system, we create the "System Construction Module" in the first phase of development. We take into account a network environment with a single base station (BS) and a huge number of wireless sensor nodes.
- The sink node acts as the coordinator's starting point. The network area is virtually divided into contiguous rings based on the location of the BS, with the width of each ring equal to the range of transmission of sensor nodes. The network is a densely deployed WSN in the sense that there are sensor nodes in each of the rings adjacent to each node, and ii) there are sufficient sensor nodes in each ring to build a routing path along the ring.
- The network model can be easily extended to accommodate scenarios with more than one BS, each of which would communicate with its corresponding sensor nodes using orthogonal frequency-division multiple-access (OFDMA). Each sensor needs to be able to collect data and identify duplicates. Every time a sensor completes a data cycle, it sends its findings to the "sink node" via a series of intermediate nodes.
- To allow any node to be chosen as a witness, the buffer space must be large enough to store the secret data of all source nodes. As new data arrives at the sensor node, the oldest data will be discarded until space is available in the buffer.

The ERCD Protocol

- In this section, we present our ERCD protocol, a distributed clone detection method that requires few buffers and has a low impact on the lifetime of the network.
- There are two phases to the ERCD protocol: choosing witnesses and checking their credentials. Each source node uses a random mapping function to choose its witnesses at random during the witness selection process. During legitimacy verification, the source node sends out a verification request to its witnesses that includes the source node's sensitive data. Once witnesses have received the verification messages, they will forward them to the witness header for legitimacy verification. The witness header is the node responsible for determining whether or not the source node is legitimate by comparing the collected messages from all witnesses. The witness header will notify the sink of a clone attack and initiate a revocation process if the received messages do not match the existing record or have expired.

Clone Detection Probability

- In this lesson, we'll look at how to design a distributed clone detection protocol with random witness selection by balancing the likelihood of finding a clone, the expected lifespan of the network, and the capacity of any data buffers. At first, only a handful of nodes are taken over by bad actors. Using the clone detection protocol, we seek to maximize the clone detection probability or the likelihood that a cloned node will be discovered; simultaneously, sufficient energy and buffer storage capacity for data collection and operating the clone detection protocol should be guaranteed, which means that the network lifetime, or the time from when the network is first activated until the first outage occurs, should not be irrationally short.

• The clone detection probability in a randomly selected set of witnesses for a distributed clone detection protocol is dependent on the likelihood that those witnesses will actually receive the verification message from the source node. Therefore, ERCD's clone detection probability protocol refers to the likelihood that the verification message will be delivered successfully from the source node to its witnesses.

• In order to ensure the safety of the network, the ERCD protocol broadcasts the verification message whenever it is in close proximity to the witness ring.

Power Use and Longevity of a Network

• Since wireless sensor nodes in WSNs are typically powered by batteries, it is crucial to assess the energy requirements of sensor nodes and guarantee that normal network operations will not be disrupted in the event of a node failure. For the purpose of measuring the efficacy of the ERCD protocol, we define the network lifetime as the time span between the first moment of network operation and the occurrence of any node outage.

• With reception accounting for such a small share of overall power usage, we focus solely on transmission power consumption. Due to the ring-based nature of the generation of witness sets in our ERCD protocol, sensor nodes within the same ring perform similar functions. The analysis is simplified by assuming that all sensor nodes within the same ring experience the same volume of traffic.

• Our work here is generic in that it can be applied to a wide range of energy models, and this is one of its main selling points. Nodes in rings with indices less than or equal to k are considered to be inside the ring, while nodes in rings with indices greater than or equal to k are considered to be outside the ring. In order to calculate energy consumption and network lifetime, we first examine the traffic load of each sensor node. Using the ERCD protocol, the typical data collection, witness selection, and authenticity verification tasks are distributed evenly across all sensor nodes.

IV. CONCLUSION

In this paper, we propose a distributed, low-energy protocol for detecting clones by randomly selecting witnesses. We have proposed the ERCD protocol, which involves the steps of selecting witnesses and verifying their credibility. Since each sensor node's witnesses are dispersed in a ring structure, detecting a clone attack is straightforward via verification message, as shown by our theoretical analysis and simulation results. In addition, with a sufficient amount of data buffer, our protocol can extend the life of the network and reduce the total amount of energy used. This is because we make use of the location data to disperse the traffic load across WSNs, relieving the burden on the sensor nodes near the sink node's energy consumption and memory storage while simultaneously increasing the network's lifespan. As we move forward, we plan to take into account a wide range of mobility trends across numerous network configurations.

V. FUTURE WORK

In the future, we will take into account varied mobility patterns across a range of network conditions in our upcoming work. The ability to encrypt packets as they are being transferred to the destination can also be added, enhancing security and reducing the risk of internal attacks brought on by network sensor nodes.

VI. REFERENCES

[1]. Z. Zheng, A. Liu, L. X. Cai, Z. Chen, and X. Shen, “ERCD: An energy-efficient clone detection protocol in wasns,” in Proc. IEEE INFOCOM, Turin, IT, Apr. 14- 19 2015, 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. 2013.

[3]. Christo Ananth, A.NasrinBanu, M.Manju, S.Nilofer, S.Mageshwari, A.PeratchiSelvi, “Efficient Energy Management Routing in WSN”, International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE), Volume 1, Issue 1, August 2012,pp:16-19

[4]. 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. 2011.

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

[6]. Uma Vasala and Dr. G. R. Sakthidharan,” Effective Key Management In Dynamic Wireless Sensor Networks”..”International Journal of Computer Engineering in Research Trends., vol.4, no.7, pp. 308- 312, 2017.

[7]. K.MANIMALA and .RANJITH,” Mobile Transmission Using Rigorous Data for Wireless Sensor Networks”..”International Journal of Computer Engineering in Research Trends., vol.1, no.6, pp. 436- 446, 2014.

[8]. P. G. V. SURESH KUMAR1 , SEELAM SOWJANYA,” Developing An Enterprise Environment by Using Wireless Sensor Network System Architecture”..”International Journal of Computer Engineering in Research Trends., vol.2, no.10, pp. 902- 908, 2015.

[9]. JALAGAM NAGAMANI, K.SUMALATHA,” EAACK: Secure IDS for Wireless Sensor Networks”..”International Journal of Computer Engineering in Research Trends., vol.1, no.6, pp. 461- 469, 2014.

[10]. G V N LAKSHMI PRIYANKA, TELUGU KAVITHA, B SWATHI and P.SUMAN PRAKASH,” Significance of DSSD towards Cut Detection in Wireless Sensor Network”..”International Journal of Computer Engineering in Research Trends., vol.2, no.1, pp. 8-12, 2015.

Cite this article as :

Sana Afia, Dr. B. Sasi Kumar, "Wireless Sensor Networks with Efficient Clone Detection in Terms of Energy and Memory", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 9 Issue 5, pp. 240-247, September-October 2022.

Journal URL : https://ijsrset.com/IJSRSET229540