International Transactions on Electrical Engineering and Computer Science
Bhargavi, Vol: 2, No: 3, pp: 112-117, Sep 2023

Providing Authenticity and Integrity for Disseminated Data Items in Wireless Sensor Networks

Bhargavi Peta*

Abstract: A Wireless sensor Network (WSN) may also be a wireless network comprising a number of sensor nodes and is used to monitor both the environmental and physical status of a given area. WSN constitute one of the most important technologies in each of the most important applications. Unit of measurement for WSN that are susceptible to security risks. Multiple Protocols are being developed to make them secure. The protection of sensitive information is the primary focus of many of the protocols that make up the major. The term given to these protocols is the knowledge discovery and dissemination protocols. Distributing management instructions and changing configuration settings on sensor nodes is accomplished with the help of the data detection and distribution protocol for WSN. Each and every one of the currently used protocols for the discovery and distribution of information has two major shortcomings. To a large extent, they encourage a centralized method (only extremely inexpensive stations are able to disseminate data item), and this is the case. This strategy is not suitable for situations in which there are numerous owners and various users. Second, security was not a consideration throughout the development of the protocols. This article proposes the first distributed information detection and distribution protocol, known as DiDrip, that is more secure than existing ones. The protocol allows numerous homeowners to authorize several network users with entirely different priorities simultaneously and immediately flow into information items to sensor nodes. This may be done by multiple homeowners simultaneously using the same protocol.

Keywords: Wireless sensor network, Sensors, DiDrip protocol

1. Introduction

The WSN is a visibly dispersed network of all tiny and light weighted nodes, which may be disseminated around the system in huge numbers depending on the measurement of various physical characteristics such as pressure, temperature and relative humidity [1].

Article History
Received: 25-06-2023; Revised: 23-07-2023;
Accepted: 28-07-2023

*Corresponding author: Department of Computer Science, Bradley University, 1718 west barker avenue Peoria Illinois, United States

E-Mail: bpeta@mail.bradley.edu

Each node in the sensor network is comprised of three different subsystems, namely the sensor subsystem, which is accountable for sensing the surrounding atmosphere, the processing subsystem, which is responsible for performing local calculations on the detected data and the communication subsystem, which is responsible for replacing messages with other nodes in the network. Occasionally referred to as a wireless sensor and actuator network (WSAN), a WSN is made up of self-sufficient sensors that are spatially allotted and used to monitor environmental or physical conditions. These conditions can include temperature, sound, and stress [2]. The sensors work together to license their information through the system to a central area. The most contemporary networks are bi-directional, which also enables the user to manage the amount of attention paid to sensors [3]. The creation of WSN was

spurred by means of army programs consisting of battlefield surveillance. Nowadays, such systems are utilized in various manufacturing and customer programs, including business progression checking and control, machine power tracking, and many others [4]. "Nodes" are the building blocks of the WSN. These "nodes" might range from a limited to many masses or even heaps, and each node is associated to one (or sometimes several) sensors. Every sensor network nodes generally consists of many components, including a radio transceiver with an internal antenna or a link to an peripheral antenna, a microcontroller, a digital circuit for interacting with the sensors, and a power source, which is typically a battery or an integrated form of power harvesting.

Even though fully functional "motes" of really tiny proportions have not yet been developed, the size of a sensor node may range from that of a shoebox all the way down to that of a particle of dust. This is the case even if the size of a shoebox is the largest. Similarly, the price of sensor nodes may range anywhere from a few dollars to several hundred dollars depending on the level of sophistication of the individual sensor nodes. Constraints on the size and cost of sensor nodes lead to comparable limitations on resources like as energy, memory, computing speed, and communications bandwidth. WSNs may have topologies ranging from a straightforward famous person community to a complex multi-hop wireless mesh network. It's possible that routing or flooding will be used as the method of propagation between the hops in the community [5]. Because of the approach's reliance on a single point of failure, information cannot be disseminated if either the base station is not operational or the link between the base station and a node is disrupted. Unfortunately, this is a single-point failure technique. The centralized solution is not only ineffective, but it is also not scalable, and it exposes users to the possibility of security breaches that might occur at any point along the path of the dialogue [6]. Even worse, some WSNs do not have any base stations at all, making them completely useless. For a WSN that is tasked with detecting illegal agricultural growing in a distant place or people trafficking at the border of a country, a base station might become an alluring target for an assault. When it comes to these types of networks, it is preferable for authorized network consumers to complete the process of data dissemination in a distributed manner. In addition, dispersed information discovery and dissemination are becoming increasingly important aspects of WSNs [7]. This is particularly true in the emerging setting of shared sensor networks, in which the sensing and communication infrastructures of a few different owners may be shared by means of programs developed by a few different users. In this protocol, dispersed operation among network owners and users with varying rights will be a major issue, but effective solutions for this problem have not yet been found.

The remaining article is structured as follows. Section 2 presents the related work, Section 3 about the framework overview, section 4 about experimental findings and lastly the section 5 discusses the conclusions.

2. Review of recent research works

Data distribution inside wireless sensor networks is an extremely important and difficult topic. The concept of a traditional communication device, in which there is a sender and a receiver, serves as the foundation for it. The scenario consists mostly of a transmitter sending out certain statistics and a receiver receiving the information that has been transmitted, processing it, and giving back a few records. Only a portion of this principle is put into practice when it comes to data distribution. Regarding the holiday destination, several inquiries are made, and information is gathered, but no response is received. The transmitter distributes the data now not to a single node but to a number of nodes, similar to a broadcasting device. In a proposal by D. He, S. Chan, S. Tang, and M. Guizani, the identities of the security flaws that may occur in the process of information discovery and dissemination while WSNs are in use were presented [6]. It allows an adversary to supplant a community with unfavorable ideals and remove important aspects. This study offers the design, evaluation, and implementation of a secure protocol called SeDrip for discovering and distributing information in WSNs. This protocol is intended to solve the weaknesses that have been identified. This protocol takes into consideration the limited assets of sensor nodes, the possibility of packet loss, and the possibility of out-of-sequence packet delivery. It is able to give instant authentication, delay the process without using packet buffering, and endure node

intrusion [7]. These are the kinds of studies that John Paul Walters, have conducted about WSN. They are looking for an efficient protective mechanism. Because a sensor network may also interact with sensitive data and operate in hostile unattended environments, security considerations must be taken into account from the very beginning of the device design process [8]. They had hypothesized that the protection provided by Wireless Sensor Networks (WSNs) would outline the requirements and constraints associated with sensor security. Smart devices like Ritu Sharma's, Yogesh Chaba's, and Yudhvir Singh's that are powered by little energy, don't cost much money, and have limited processing capacity are part of WSN [9]. Because there may be a considerable development in the usefulness of wireless sensor networks, the safety measures are also likely to become an increasingly significant challenge. The Wireless Sensor Network has already been used to implement a wide range of real-world utilities all around the world. These types of programs are available: monitoring of geographical areas, medical treatment, manufacturing, transportation, military activities, tracking of the environment, monitoring of industrial machinery, and surveillance systems [10]. the typical limits, security dreams, chance models, and standard assaults on sensor networks, as well as their protective strategies or countermeasures relevant to the sensor networks based on the notion of those parameters that the researchers had completed. They established the first methodology that was loosened and authorized for the finding and distribution of data. It will enable the network owner to authorize more than one network consumer with the particular rights to the sensor node, which will allow the statistics items to be disseminated concurrently and without delay [11]. Additionally, it will solve a variety of safety vulnerabilities that may potentially occur. Archana Taal, Prachi, the findings of these investigations suggest the following: Applications within the wireless sensor community are expanding daily [12]. Data nodes within the sensor community are simple to acquire, and eavesdroppers can access the confidential information stored inside sensor nodes. Wireless communication has always been known to have difficult security measures. The safety of WSNs relies heavily on the techniques used in cryptography [13]. In order to show a security method for WSN that is both power efficient and challenging to crack, they propose a novel symmetric key algorithm that is entirely based on shuffling, replacement, and transferring. This algorithm is the heart of their protection scheme. The capabilities include the amount of time required by the algorithm for an exceptional key size and the number of rounds, in addition to a comparative assessment of the suggested set of rules with AES on a variety of parameters to demonstrate its effectiveness [14].

3. Frame work design

A wireless sensor network, also known as a WSN, is comprised of independently operating sensors dispersed throughout a given area. These sensors monitor environmental or physical factors, such as temperature, sound, or pressure, and then share the data they collect with one another before transmitting it to a central point. The most cutting-edge networks are bi-directional, which enables control of sensor activity in addition to other benefits. Military applications such as battlefield surveillance were the impetus for the development of wireless sensor networks. These days, such networks are employed in a variety of industrial as well as client applications, such as process observation and management, machine vigor observation, and so on.

3.1 System Overview

The DiDrip protocol is broken down into four stages: the system format, user joining, packet pre-processing, and packet verification. In the portion of the system formatting that pertains to our fundamental protocol, the network owner generates both public and private keys for the network, and then populates the general public parameters on each node prior to the deployment of the network. A user obtains the dissemination permission after they have joined the network and registered with the network owner. If a user connects to the network and has to disseminate any data items, that user should create the information dissemination packets.

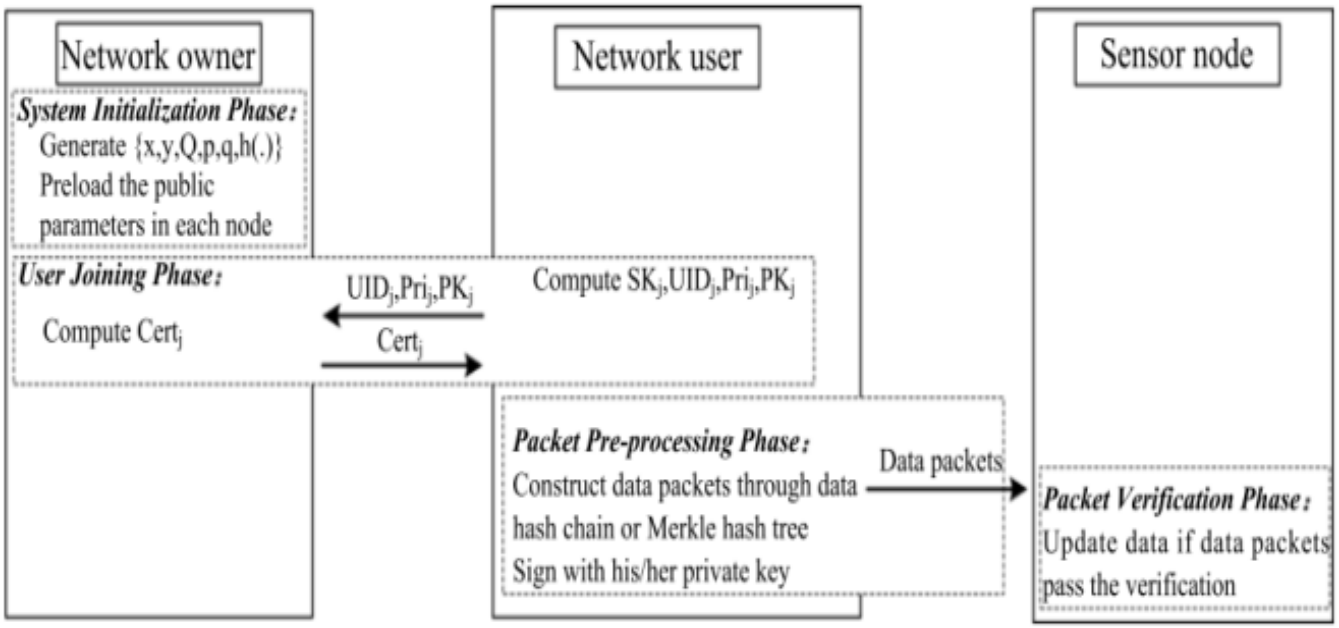

Fig.1: Proposed wireless sensor network

So that they may transmit them to the nodes in the network during the stage of the process known as packet pre-processing. During the stage of the process known as packet verification, a node checks each incoming packet. In the event that the test is successful, the information is modified in accordance with the received packet. They offer DiDrip as a solution, which shows that they support the planning aims. It is the fundamental protocol for the discovery and distribution of dispersed information. It enables network owners and other authorized users to import data items into WSNs without having to depend on the base station. In addition, our comprehensive research reveals that DiDrip complies with the prerequisites for safety imposed on protocols of its type. To be more specific, they use the common security method to explicitly demonstrate the authenticity and integrity of the data items sent over DiDrip.

3.2 DiDrip Protocol modules

The DiDrip have 3 main modules,

1. Create Network Module
2. User Privileges Module
3. Packet verification Module

Create Network

The proprietor manages this module, and a large number of users may access it. The sensor nodes' memory space, computing capabilities, bandwidth, and power supply are normally within the controller's discretion. Consequently, when its battery is functional, a sensor node can only carry out a certain amount of activities using public key cryptography.

Access rights of users

Within the context of this module, the network administrator or network owner can confer a certain degree of authority on each user. For instance, a user may only disseminate data items to a set of sensor nodes with specified identities and/or in a specific localized region. This restriction applies to both the user and the sensor nodes.

Packet verification

The packets need to be inspected for this particular module. Checking the key field of a packet is something that a sensor node does whenever it gets a packet, regardless of whether the packet came from an authorized user or from its neighbors on the same hop.

4. Experimental results

User privilege, which is regulated in this experiment by the user certificate, may be used to limit the functions that network users are able to perform. If privilege is changed after a user certificate has already been created, the signature verification process at sensor nodes will fail to authenticate the certificate as legitimate. Therefore, only the network owner can modify the privilege, and they are also the only ones who can update the certificate.

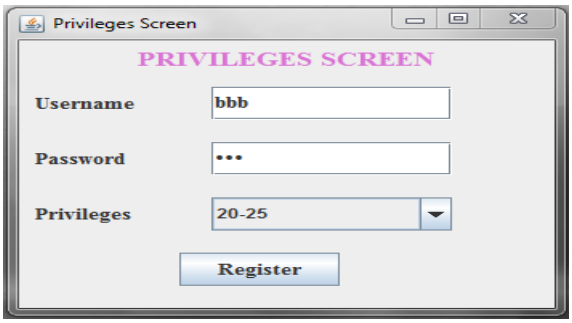

Fig. 2: Privileges screen

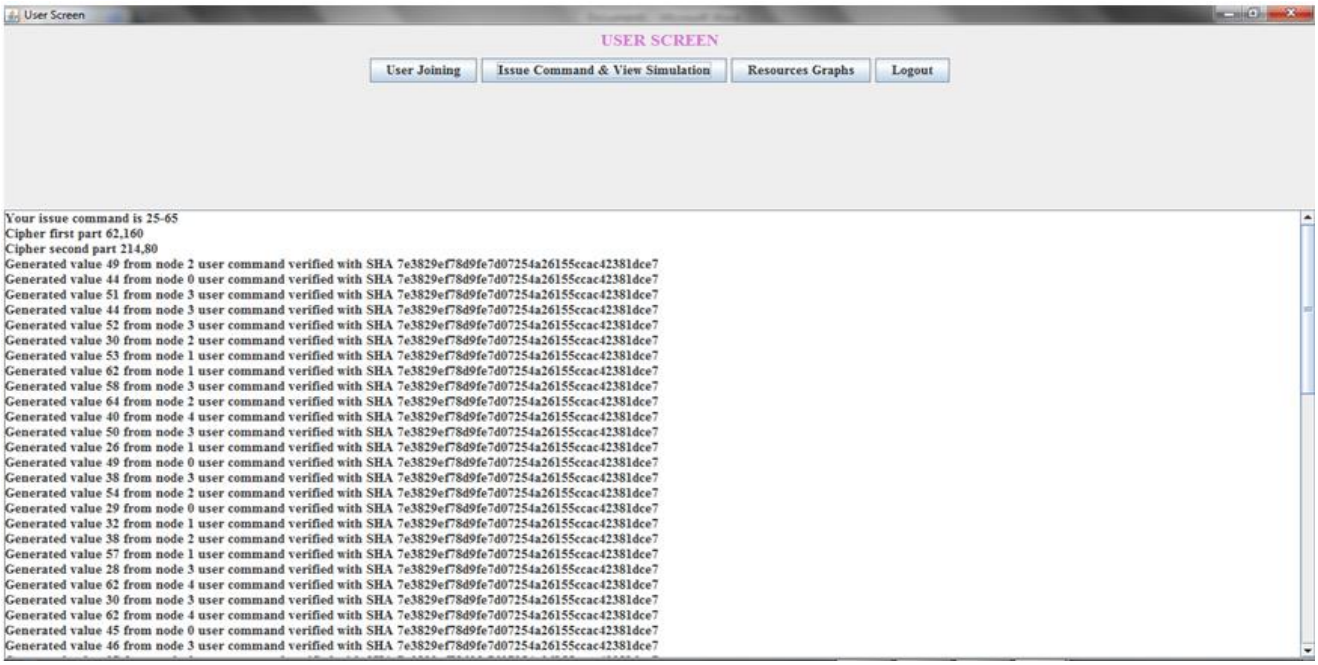

Fig. 3: User screen with output data

Each user is required to provide the owner of the network with both their private key and their dissemination permission when registering with the network. This is necessary so that the signature verification of the sensor nodes may be passed. Within the framework of this protocol, the commands will be broken up into a first part cipher and a second part cipher. The SHA algorithm will be used to do the verification of the directives. By using this SHA algorithm, we are able to increase both the authenticity and integrity of the data items that are disseminated over wireless sensor networks.

5. Conclusion

Our findings lead us to the conclusion that, throughout the course of this work, we hypothesized that a safe and distributed data discovery and dissemination protocol called DiDrip has been developed. In addition to investigating how DiDrip may be protected, the authors of this study provide the findings of an investigation into how DiDrip operates in an empirical network of resource-constrained sensor nodes. These findings demonstrate that DiDrip can be implemented in real-world settings. In addition to this, we have provided an adequate confirmation of the validity and integrity of the data

items that have been sent over DiDrip. In addition, messages may be easily intercepted owing to the open nature of wireless channels, which allows for their use.

Conflict of Interest

The authors declare "No conflict of interest"

References

[1] N. Vipul, A. K. Daniel and P. Chaturvedi "E-FEERP: Enhanced Fuzzy based Energy Efficient Routing Protocol for Wireless Sensor Network." *Wireless Personal Communications*, pp.1-28, 2023.

[2] S. Vikrant, S. Vats, D. Arora, K. Singh, A. S. Prabuwono, M. S. Alzaidi and A. Ahmadian. "OGAS: Omni-directional Glider Assisted Scheme for autonomous deployment of sensor nodes in open area wireless sensor network." *ISA transactions*, Vol. 132, pp. 131-145, 2023.

[3] T. Natalie, C. Sergiou, C. Georgiou and Vasos Vassiliou "A survey on mobility in wireless sensor networks." *Ad Hoc Networks*, Vol. 125, art.no: 102726, 2022.

[4] S. Neelakandan, P. Mohan, Y. Alotaibi, S. Alghamdi and O. A. Khalaf "An efficient metaheuristic-based clustering with routing protocol for underwater wireless sensor networks", *Sensors* Vol. 22, No. 2, pp. 1-15. 2022.

[5] J. W. Hui and D. Culler "The dynamic behavior of a data dissemination protocol for network programming at scale," *Proceedings of 2nd International Conference on Embedded Networked Sensor Systems,* pp. 81–94, 2004.

[6] D. He, C. Chen, S. Chan, and J. Bu "DiCode: DoS-resistant and distributed code dissemination in wireless sensor networks," *IEEE Transactions on Wireless Communications*, Vol. 11, No. 5, pp. 1946-1956, 2012.

[7] T. Dang, N. Bulusu, W. Feng, and S. Park "Dhv: A code consistency maintenance protocol for multi-hop wireless sensor networks." *In Wireless Sensor Networks: 6th European Conference*, Cork, Ireland, February, pp. 11-13, 2009.

[8] G. Tolle and D. Culler "Design of an application-cooperative management system for wireless sensor networks," *Proceedings of the Second European Workshop on Wireless Sensor Networks*, pp. 121–132, 2005.

[9] K. Lin and P. Levis, "Data discovery and dissemination with DIP," *In 2008 International Conference on Information Processing in Sensor Networks*, pp. 433-444, 2008.

[10] M. Ceriotti, G. P. Picco, A. L. Murphy, S. Guna, M. Corra, M.Pozzi, D. Zonta, and P. Zanon, "Monitoring heritage buildingswith wireless sensor networks: The Torre Aquila deployment," *2009 International Conference on Information Processing in Sensor Networks*, pp. 277–288, 2009.

[11] D. He, S. Chan, S. Tang, and M. Guizani, "Secure data discovery and dissemination based on hash tree for wireless sensor networks," *IEEE transactions on wireless communications,* Vol. 12, No. 9, pp. 4638–4646, 2013.

[12] M. Rahman, N. Nasser, and T. Taleb "Pairing-based secure timing synchronization for heterogeneous sensor networks," *2008 IEEE Global Telecommunications Conference,* pp. 1–5, 2008.

[13] P. Levis, N. Patel, D. Culler, and S. Shenker, "Trickle: A self-regulating algorithm for code maintenance and propagation in wireless sensor networks," *In First USENIX/ACM Symposium on Network Systems Design and Implementation*, pp. 15–28, 2004.

[14] Y. Chen, I. Lin, C. Lei, and Y. Liao, "Broadcast authentication in sensor networks using compressed bloom filters," *In Distributed Computing in Sensor Systems: 4th IEEE International Conference,* pp. 99–111, 2008.

***