A SURVEY ON SECURE DATA DISSEMINATION IN WSN

K. SAI PRIYA,[1]Student,
P.SREEKANTH[2], Assistant Professor,
Electronics and Communication Department,
CVR College of Engineering, Hyderabad,Telengana,India.

Abstract—A Wireless sensor network (WSN) is a network together with sensor nodes that connected through wireless media. After deploying a WSN, it may be necessary to update or change some common variables such as sensing interval, data sending interval or small programs stored in each node of the network. It is not always feasible to update sensor nodes in the ad-hoc fashion manual. We, therefore, use data dissemination protocols to change the parameters of the sensor setup. Existing data discovery and dissemination protocols endure two essential disadvantages. In the first place, they depend on the unified methodology; in this methodology, the main base station can scatter data things. Such a methodology experiences a solitary purpose of disappointment. Second, most protocols assume that the working environment is safe, so attackers can easily harm the network. In Wireless Sensor Network (WSN) security and confidentiality on data are most important aspects. This paper proposes a secure and distributed data dissemination protocol named Sec-DiDrip. It encourages the direct dissemination of data items to the sensor nodes by multiple authorized network users. Sec-Drip enhances security for the confidentiality of disseminated data.

Keywords: Wireless sensor networks(WSN)***, security threats, distributed data, sec-didrip.***

I.INTRODUCTION

A Wireless Sensor Network (WSN) comprises of self-sufficient spatially disseminated sensors for checking physical or ecological conditions, for example, temperature, sound, and weight and so on to helpfully go their data through the network to an area. Military applications, for example, front line reconnaissance have empowered the development of wireless sensor networks and are in this way utilized in numerous mechanical and customer applications, for example, modern procedure checking and control, machine wellbeing observing, and so forth.

A sensor network comprises of different recognition stations, every one of which is little, lightweight and versatile, called sensor hubs. Every sensor hub has a transducer, microcomputer, handset, and a vitality source. The transducer uses sensed physical impacts and phenomena to generate electrical signals. The microcomputer procedures and stores the sensor yield. The handset gets directions from a focal PC and transmits data to that PC. A battery derives the energy for each sensor node.

The way sensor nodes sense the data packets and transfer it over some intermediate nodes to the root or base station [1]. Low cost, low energy, and a short-range of transmission are the sensor nodes. Nodes use to send data parcel of data packets locally to its single-bounce neighbor nodes etc. lastly it compasses to its base station. At first, nodes are conveyed flying from air ship or arbitrarily and at some point, hub changes its underlying position (the season of organization) and moves over the locale dependent on the necessity; along these lines, this kind of hub is called versatile nodes. In this way, there are two kinds of data transmission in wireless sensor networks, these are – direct transmission and multi-bounce data transmission. Backhanded transmission, data are sent straightforwardly to the sink though multi-bounce transmission data send by means of no of middle of the road nodes lies between the source hub and base station.

With their safety and reliability, the ad hoc nature of sensor networks presents unique challenges. Limited memory resource sensor nodes; low energy, restricted processing capacity, and low coverage are vulnerable to intrusion, interception, modification, and fabrication. On account of these one of a kind difficulties customary security system are insufficient to meet the security objectives of Confidentiality, Integrity, Authentication, and Availability (CIAA).

- Confidentiality is the capacity to hide message from a latent assailant, where the message imparted on sensor networks stay classified.
- Integrity relates to the capacity to verify that the message was not modified, altered or changed while on the network.
- Authentication needs to know if the messages are the node it claims to be from, determining the reliability of the message's origin.
- Availability is to decide if a hub has the ability to utilize the assets and the network is open to carry on the messages.

Data Confidentiality:

Data confidentiality is the ability to conceal an attacker's network traffic so that any communication via the sensor network remains secret and is the key issue of network security. In many applications (like key distribution) nodes communicate secret and highly sensitive data. The common strategy to maintaining sensitive data secret is to encrypt it with a secret key that only authorized receivers to possess, thus attaining confidentiality.

Public-key cryptography is very expensive to use in resource-constrained sensor networks, so most of the protocols proposed to use symmetric key encryption techniques. Moreover, confidentiality just ensures the security of correspondences inside the sensor network, it doesn't avoid the abuse of data that arrives at the base station. It is therefore required that information must be

coupled with the right control policies so that unauthorized users can be prevented from having access to confidential information.

WSNs are mainly used for tracking and monitoring applications. After WSN is deployed, configuration parameters or old programs in each node are required to be updated. This process is called as data discovery and dissemination. Data dissemination aims to send any types of information (data or query) to all nodes when minimizing the number of forwarding nodes and energy cost. Dissemination facilitates a source to inject configuration parameters, queries, commands into the sensor node. But an adversary can change the data that is being disseminated or forge a data item. Hence various security mechanisms need to be implemented to protect the data from the attacker.

Some WSNs have no base station at all. For example, for a WSN monitoring human trafficking in a country's border or a WSN deployed in a remote area to monitor crop cultivation, a base station becomes an attractive target to be attacked. For such networks, information dissemination should be carried out in a distributed way by approved network users. A system overview of centralized and distributed data discovery and dissemination approaches is presented in fig.1:

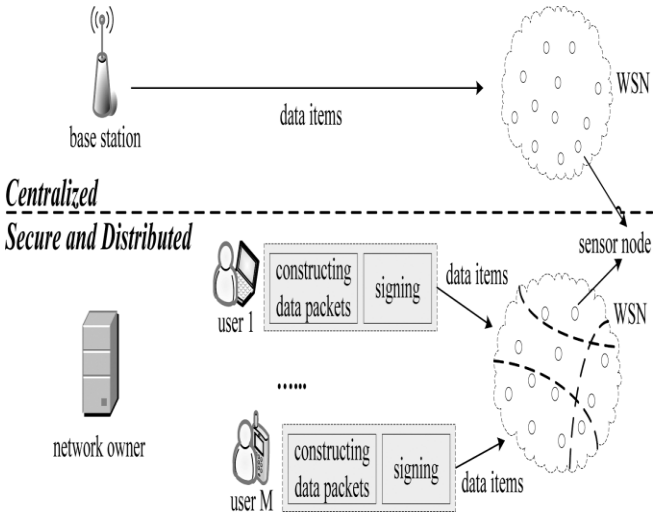

Figure 1: System overview of centralized and distributed data discovery and dissemination

Fig.1, only the base station can disseminate data items. Tragically, this methodology experiences the single purpose of disappointment as dissemination is unthinkable when the base station isn't working or when the association between the base station and a hub is broken. Furthermore, the centralized strategy is inefficient, non-scalable and vulnerable to security threats that can be initiated along the communication route anywhere.

II. LITERATURE SURVEY

In literature survey, several data dissemination protocols are in existence.

A. DRIP

Tolle et al. Presented Sensor Network Management System (SNSM), which is an application – cooperative management system for WSN and Drip is the dissemination protocol which is employed in it [2]. Drip is the most straightforward of all dissemination protocols and relies upon stream rule and sets up an independently employed stream for every factor inside the learning. Each time an application needs to transmit a message, a substitution adaptation id is created and utilized. This can make the convention reset the Trickle clock and henceforth spreads the new worth. Drip gives an average message gathering interface in WSN. Drip accomplishes adequacy by keeping away from excess transmissions if a proportional data has just been gotten by the nodes inside the area.

MERITS:

It avoids redundant transmission and achieves greater efficiency.

B. CODEDRIP

It is a data dissemination protocol proposed by Nildo et al. and can be employed in wireless sensor networks [3]. This convention is particularly utilized for dissemination of little qualities. Network committal to composing is an instrument that blends bundles in the network which would expand the out turn and abatement number of messages transmitted. CodeDrip uses network Coding to improve the unwavering quality and speed of dissemination. CodeDrip utilizes the Trickle rule for dissemination. It resembles Drip separated from the very reality that here messages are once in a while consolidated and sent. To blend messages, coding protocols utilize totally various administrators, here XOR administrator is utilized.

MERITS:

Use of network coding increases throughput and decreases number of messages transmitted and thereby improves reliability and speed of dissemination.

C. *DIP*

DIP (Dissemination Protocol) is known as data detection and dissemination protocol as defined by Lin et al [4]. It works in two sections: location whether a distinction in data in nodes has happened and separating that data thing is totally unique. It utilizes the idea of rendition assortment and keys for each datum thing. DIP uses stream calculation to ascertain and send hashes that check all the form numbers. DIP likewise deals with a delicate state gauge of whether a given thing varies from a neighbor's thing or not.

MERITS:

It distinguishes difference of data in a node and identifies the different data items. The version or tag number with keys for each data packet or item is used.

D. DHV

DHV is a code consistency overseeing convention proposed by Dang et al [5]. The name DHV starts from three stages in the convention – Difference discovery, Horizontal hunt and Vertical inquiry. It attempts to keep up codes on totally various nodes during a WSN, steady and forward-thinking. Here data things are portrayed as tuples (key, variant). This convention attempts to compensate for the weaknesses of past protocols like DIRP and DIP by lessening the quality worry inside the refreshing of data in the network. Here the rendition number is given as a bit exhibit. DHV uses bit cutting to rapidly confirm the out of data code, prompting less bits being transmitted inside the network. DHV incorporates two essential stages: discovery and distinguishing proof. In discovery, each hub can communicate a hash of every one of its variants during a framework message. After getting this, a hub looks at it to its hash. On the off chance that they are not comparative, there is one or a great deal of code things with a unique rendition number. In recognizable proof, the even hunt and vertical pursuit steps are acclimated deciding the distinction in the adaptations.

MERITS:

This convention of protocol attempts to beat the bad marks of past protocols like DRIP and DIP by diminishing the issues associated with the refreshing of data and its uses bit cutting of variant numbers in the network.

E. TYPHOON

The data is rigid and reliable data dissemination protocol utilized in wireless sensor networks (WSN) given by Liang et al [6]. It is predominantly used for dissemination of large data like Deluge. Therefore, in this case as well massive data objects are divided into fixed sized pages or packets. In contrast to different protocols, typhoon sends data packets in unicast fashion. This methodology grants beneficiaries to recognize the receipt of bundles and subsequently rapidly recuperate lost parcels assuming any. While data bundles are sent in unicast way, intrigued nodes will get those parcels by snooping on the wireless medium. Along these lines, through the blend of unicasting and snooping, this convention accomplishes brief retransmission and data conveyance to any or every one of the nodes during an area through one transmission. Tropical storm uses stream clocks for dissemination of meta-data. Here meta-data incorporates object ID, size and form to point the presence of a crisply made data object.

MERITS:

It utilizes a blend of spatially tuned clocks, brief retransmissions, and recurrence assorted variety to diminish dispute and as often as possible decent variety to decrease conflict and advance spatial re-use and furthermore lessen dissemination time and vitality utilization.

F. MNP

Sandeep et al. anticipated a Multi-bounce Network reconstructing Protocol (MNP) [7],[8]. It gives a solid support of engender new program code to all sensor nodes inside the network. The essential target of this dissemination convention is to affirm solid, low memory use and speedy information dissemination. It depends on a sender decision convention inside which supply nodes complete with each other dependent on the quantity of particular solicitations they have gotten. In each area, a source hub conveys program code to numerous beneficiaries. When the collector gets the total program picture next to them, they become source nodes, and send the code into their neighborhood. Pipelining is regularly included during this convention to empower speedier information proliferation inside the instance of bigger networks. To do pipelining, programs are isolated into fragments, every one of these portions contain a fixed number of parcels. When a finder hub collector every one of the portions of a program, it will reboot with the new program.

MERITS:

It provides reliability, low memory usage and fast data transfer.

G. DIDRIP

DiDrip is the data dissemination protocol which discovers and disseminates the data in secure and distributed manner. Literature survey shows that all existing protocols are based on centralized approach. It means data can be disseminated in the node by the base station only. This type of approach fails when the working of base station fails or connection between base station and other nodes is damaged. Another drawback of existing system is, the protocols developed assume that the outside environment is secure. But DiDrip is the first protocol which is designed by taking security in mind and is based on distributed approach. In this type of approach multiple authorized users get privilege to disseminate the data in the network.

MERITS:

ECC cryptography is used for key generation and to make it more secure Hash function is used.

DRAWBACKS:

DIDRIP comprises a network owner, users and sensor nodes. Network owner has a public-private key pair. Each network user gets a certificate after registering with the network owner. Users also have a public private key pair and dissemination privilege. When user needs to disseminate data, he will construct the packet and signs with his private key. User certificate is also transmitted along with acknowledgement packet. There are some efficiency problems with this DIDRIP. It is not efficient in communication since the certificate need to be transmitted with the advertisement packet.

The algorithm used so far is the algorithm TRICKLE. It's an algorithm that self-regulates. It is expensive to propagate code; it is even more expensive to learn when to propagate code. Bits should occasionally convey to realize when there is another code. To decrease vitality costs, bits can transmit metadata to decide when the code is required. Trickle, an algorithm used in wireless sensor networks to propagate and maintain code updates. Its −Polite Gossip based.

III. PROPOSED METHOD

Sec-DiDrip allows multiple authorized network users to directly disseminate data items to the sensor nodes. Sec-Drip enhances security for the confidentiality of disseminated data. Each node in the WSN should receive a copy of disseminated data. For this, the Trickle algorithm is used, which is used by most dissemination protocols. In order to ensure the freshness of the data version number is used. Each data item is identified by the tuple (key, version, and data). Since sensor nodes are resource-limited devices a lightweight block cipher encryption algorithm is used for encrypting the disseminated data. The algorithm used is based on chaotic maps and genetic operations which is suitable for a wireless environment. The proposed Sec-DiDrip contains of 4 phases like system initialization, user joining, packet preprocessing and packet verification.

A. SYSTEM INITIALIZATION

The network proprietor makes its open and private keys, and afterward stacks the open parameters on every hub before the network arrangement were carried over.

B. USER JOINING

A user gets the privilege of dissemination by registering with the owner of the network.

C. PACKET PRE-PROCESSING

On the off chance that a client enters the network and needs to scatter certain data things, the data dissemination bundles should be built and afterward sent to the nodes.

D. PACKET VERIFICATION

A node verifies or checks each packet got received or not. If the outcome is positive, the received packet will update the data.

Sec-Drip combines ECC (Elliptic Curve Cryptography) and Merkle hash tree. Thus, it inherits robustness to packet loss using Trickle algorithm where there is periodic delivery of data to every node in the network.

IV CONCLUSION

The main objective of Sec-DiDrip is to solve the efficiency problems in DiDrip and enhances the security of DiDrip by ensuring the confidentiality of disseminated data. There is a lot of communication overhead due to the generation, transmission, and verification of certificate in the basic protocol. Sec-Didrip is a secure and distributed data dissemination protocol that can be used for the secure and efficient dissemination of data in wireless sensor networks.

REFERENCES

[1] Sneha Ghormare, Vaishali Sahare, "A Survey on Data Confidentiality for Providing High Security in Wireless Sensor network",International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE) Volume-5, Issue-1, , pp. 249-252, January – 2015.

[2] G.Tolle and D.Culler, "Design of an application cooperative management system for wireless sensor networks," Proc.EWSN,pp.121-132,2005.

[3] Nildo dos Santos Ribeiro Junior, Marcos A.M.Vieiral, Luiz F.M.Vieiral and Om Gnawali, "Code Drip:Data Dissemination Protocol with Network Coding for Wireless Sonsor Networks", In Proceedings of the 11th European conference on Wireless Sensor Networks(EWSN 2014) Feb,2014.

[4] Lin, K., Levis, P.: "Data discovery and dissemination with DIP:" In Proceedings of the 2008 International Conference on Data Processing in Sensor Networks (IPSN 2008), Washington, DC, USA, IEEE Computer Society (2008) 433-444.

[5] T.Dang, N.Bulusu, W>Feng, and S.Park , "DHV:A code consistency maintenance protocol for multihop wireless sensor networks", in Proc.2009 EWSN,pp. 327-342.

[6] Liang, Chieh-Jan Mike, and Andreas Terzis. "Rethinking multi-channel protocols in wireless sensor networks",Proceedings of the 6th workshop on Hot Topics in Embedded Networked Sensors.AMC,2010.

[7] Kulkarni, Sandeep S., and Limin Wang, "MNP:Multihop network reprogramming service for sensor networks" Distributed Computing Systems,2005.ICDCS 2005.Proceedings 25th IEEE International Conference on IEEE, 2005.

[8] Hailum Tan, "Secure multihop network programming with multiple one-way key chains", In:Proceedings of the International Conference on Embedded networkd sensor systems(Sensys 07), Sydney, Australia, ACM.

AUTHOR'S BIOGRAPHY

1.K.Sai Priya received the B.Tech degree in Electronics and Communication from JNTUH in 2017.Currently pursuing M.Tech from CVR College in Wireless & Mobile Communication.

2.P.Sreekanth received B.Tech. and M.Tech. degree in Electronics and Communication Engineering from Jawaharlal Nehru Technological University, Hyderabad, India. He is pursuing a Ph.D. degree in Osmania University, India in the Department of Electronics and Communication engineering. He is also Assistant Professor in the Department of Electronics Engineering, CVR College of Engineering, Ibrahimpatnam, Hyderabad, India. He has authored or co-authored over 12 research papers in international / national journals / conference proceedings. His research interests include ad-hoc wireless sensor networks, internet of things, heterogeneous networks.