International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-11, September 2019

# Sec-Didrip: A Secure Routing Protocol for Wsn Using Ns-3

**K. Sai Priya, P. Sreekanth**

***Abstract:*** ***Wireless sensor networks (WSN) are responsible on improving or updating and distributing security commands for the data discovery and the dissemination protocols to update the sensor Node configuration parameters. There are two drawbacks to all current data discovery and the dissemination protocols. First, they are based on the centralized strategy; the data item can only be distributed by the base station. For emerging multi-owner-multi-user WSNs, such a strategy is not appropriate. Furthermore, those conventions have not been proposed in view of security and in this manner, assailants can promptly dispatch endeavors to harm the system. This article proposes the first-named convention (Sec-DiDrip) for secure and circulated data discovery and dissemination.***

***Keywords: Data dissemination, distributed strategy, sec-didrip protocols.***

## I. INTRODUCTION

Wireless sensor network (WSN) has a common need to refresh parameters put away in the sensor hubs. The data discovery and the dissemination protocol give's a source to pervade small projects, commands, inquiries and design parameters into sensor hubs will accomplish this which are located in the hostile environments. Note that it is not the same as the code dissemination protocols which circulate huge doubles to reconstruct the entire system of sensors. For cite, the productive dissemination of a double document of several kilobytes (KBs) requires a code dissemination protocol.

Scattering a few two-byte setup parameters requires a data discovery and the dissemination protocol. Taking into account that the sensor hubs could be conveyed in an unfriendly domain, the remote dissemination of such little data to the sensor hubs through the remote channel is a more liked and pragmatic methodology than manual mediation. Spurred by the above perception, this paper as the accompanying essential commitment isn't completely new to the requirement for conveyed data discovery and the dissemination protocol, however earlier work did not address on the need we study utilitarian prerequisite of such protocol and said their structure objective. Also, we identify the security vulnerabilities, breaches and compliance of data in existing data discovery and the dissemination protocol.

Some data determinations and protocols of dissemination for the Wireless Sensor Network (WSNs) were recommended. Among the proposed protocols, (DHV) allows node to transmit required level of bit information, (DIP) allows each node to implicitly calculate the neighborhood node, and Drip are viewed as the best in class protocols and have been incorporated into the Tiny OS dispersions. All proposed protocols expect that the working condition of the WSN is reliable and has no enemy. Notwithstanding, enemies exist and force dangers to the ordinary task of WSNs. This issue has tended to late, by which it is distinguished the security and confidentiality of data vulnerabilities of Drip and proposes a compelling arrangement. More significantly, the brought together procedure is utilized by every single current datum discovery and dissemination protocols. Tragically, this methodology experiences single purpose of disappointment as dissemination is incomprehensible 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 susceptible to security threats that can be initiated anywhere throughout the communication path.

Linear network coding is a technique used during dissemination to achieve frequency and energy effectiveness. It is a technique that transfers packets to network; increases throughput, decreases energy consumption and decreases the number of transmitted packets. In traditional systems the dropped packets are recovered by retransmission. But we can connect packets with mathematical operations in network coding and then disseminate them to recover lost packets which are achieved without retransmission.

But network coding carries a lot of headaches along with its energy efficiency benefits. Attacks such as pollution, denial-of-service attacks, and many others are extremely susceptible. The proposed scheme, therefore, utilizes simple but effective cryptographic methods for the dissemination of data to cope with these. This ensures that in the wireless sensor networks we can accomplish simple yet secure data dissemination.

The scenario of our work is as follows. First, we concentrate on the need for the wireless sensor networks to disseminate data and some of their associated works. Next, the design and implementation that focuses on disseminating tiny values and variables are discussed. Then we use tiny OS to explore the new protocol's efficiency through comprehensive simulation and eventually have the conclusion and references.

**Manuscript published on 30 September 2019.**
***Correspondence Author(s)**
**K. Sai Priya***, Electronics and communication engineering, CVR College of Engineering, Hyderabad, India.
**P. Sreekanth*,** Electronics and communication engineering, CVR College of Engineering, Hyderabad, India

## I. RELATED WORK

Data Distribution in the remote sensor systems is a basic what's more, fundamental undertaking. It depends on the concept of conventional correspondence framework, where sender and beneficiary are present. The situation is fundamentally a sender conveys some data, and the beneficiary gathers the sent data, preparing it and sending some of the data back. While in information scattering, just 50% of this idea is connected. Some data is conveyed and got at the receiver end; however, no answer is received. The transmitter conveys the data, not only to one node, but rather to numerous as in a TV framework.

Scattering is utilized to send the code overhauls or program pictures to the sensor nodes intermittently to perform reconstructing of the nodes. The main point of a WSN dispersal convention is to ensure that predictable data is available to all sensor nodes constantly.

There are two sorts of scattering in WSN [1]: Code scattering - to transfer program pictures which are by and large massive information. Generally, they are partitioned into altered estimated pages and parcels and after that spread. Data discovery and the dissemination - to scatter little arrangement parameters, variables, inquiries, orders and so on in parcels.

### 2.1 SMALL VALUE DISSEMINATION

It concentrates on the protocols for the data discovery and dissemination, i.e. the dissemination of small values such as variables, parameters, etc. Figure 1 provides a general idea of dissemination of data. Drip, DIP and DHV are traditional protocols accessible for this purpose. They are all based on the algorithm of Trickle [2].

Drip is proposed by Tolle et. al. [3] which is the most straightforward of all dissemination protocols and depends on the Trickle calculation and sets up an independent stream for every datum variable. A new version number is produced and used whenever an application wishes to communicate a message. This will affect the Trickle timer to reset the protocol and thus disseminate the new value, otherwise, the trickle timer interval will be increased.

DIP (Dissemination Protocol) [4] is a protocol suggested by Lin et al to detect and disseminate data. It's a Trickle algorithm-based protocol. It operates in two components: to determine if there is a distinction whether data is stored at the node, and then to determine which data is distinct. It depends on the idea of variant number and a key tuple for every datum item. DIP calculates the hashes covering all data version numbers. Nodes that get hashes equivalent to their very own realize that they have reliable data as for their closest neighbors. In the event that a hub gets a hash that varies from its very own hash, and it realizes that a distinction exists in the data.

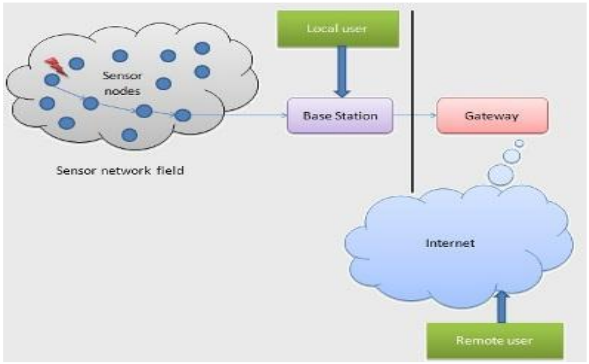


**Fig.1.WSN Example**

### 2.2 NETWORK CODING AND DATA DISSEMINATI-ON

Network coding is intended to substitute the traditional forward technique which is used in the networks; by better routing algorithms to enable intermediate nodes to convert moving data. Due to its characteristics, network coding has enhanced parameters like robustness, high security and better throughput. It helps to accomplish rapid dissemination of data as it decreases the no. of retransmissions required if packet losses occur. Many dissemination protocols came into existence that have been developed using the idea of network coding.

Dissemination protocols based on network coding have several advantages in achieving energy savings and commun -ication efficiency, particularly during enhanced packet loss or network density. Network-based coding protocols can, therefore, be beneficial for WSN reprogramming. However, in hostile environments, we face a prospective challenge. An intruder may launch the pollution attacks in which the malicious node transmits poorly encoded packets consisting of bogus or fake information, resulting in inaccurate decoding of the initial information after recovery.

## II. PROPOSED SYSTEM

Data dissemination is performed in a secure and fast manner using network coding and cryptography techniques in this protocol. Network coding decreases the number of retransmissions by combing and sending data owing to any packet loss that occurs in the network. Disseminated information is also always transmitted in form of encrypted data. First, execute or coordinate node to node authentication and create session keys for this node. Then the session key is used to encrypt the data transfer. This protocol ensures that the system is free from pollution, heavy request on controlling the Denial-of-Service attacks.
The different phases of this protocol include:

### 3.1 SYSTEM INITIALIZATION PHASE

In this stage, a primary key Km and a distinctive random number Rm are generated by the base station and securely stored in every node. All the valid node_ids lists are stored in each node.

### 3.2 PACKET PROCESSING PHASE

In this phase, the actual data dissemination process occurs. Before disseminating the data, a real-time key using key generation algorithm like PGP encryption is generated by the node. This involves the generation of the R1 node and R2 node two unique random numbers. The key is obtained by using Trivium-Multilinear Modular Hashing (TMMH) as the MAC function and SHA1 as the H(x) hashing function. The steps are:

$$1.\ MAC[i] = R1\_node\ XOR\ K[i] \quad (1)$$
$$2.\ a[i] = node\_id + MAC[i] \quad (2)$$
$$3.\ h = MMH\ (\ a[i]\ ) \quad (3)$$
$$4.\ Key = H\ (\ h\ XOR\ R2\_node\ ) \quad (4)$$

Where K[i] is the MAC function's master key, node_id is the related node identifier, XOR is the logical operation. The node broadcasts this real-time key in a packet that includes the node_id and the key. The destination node which receives the key will check the node_id within its valid node list and make sure that this packet comes from a valid node. If yes, then that node will also generate a real-time key using the same process as above and return to the sender node a reply packet containing the node id and the newly generated key.

If this packet is also validated, a session key will be generated by the two nodes. The key is generated as follows:

$$Session\ key = K_m\ XOR\ K_a\ XOR\ K_b$$

Where $K_a$ and $K_b$ are keys generated at two nodes A and B. We prefer to use the Advanced Encryption Standard (AES) strategies to encrypt the information. Therefore, the distributed data packet from a node contains the information in encrypted form i.e.

$$Data = E(d)_{sessionkey}$$

A random number one-time hash is calculated to authenticate data packets immediately and is included in each packet. The steps are

$$CHash = H(R_m)$$

Result = ADD(Hash)

### 3.3 PACKET VERIFICATION PHASE

The destination node calculates the hash of Rm which is stored in its own memory and compares it with the value it received, which is used to achieve immediate authentication of the received packet. If it matches, then a valid node is present in the received packet. Thus, the destination will acknowledge ACK. Otherwise, the sender will receive a NACK (negative ack). Next we need to guarantee the data's integrity. For the first time, the node checks the *id* in the received packet.

If this is a valid node_id, the already generated and preserved session key will try to decrypt the information. Each node has its original data buffer and a combination of data. The node will, therefore, test whether it is an original data or a combination of data. If data is original, then it will be stored and disseminated after a trickle timer fire, else it is a combination of data, which the node will verify whether any other information can be extracted using network coding from this newly gathered data. The information will then be stored or disseminated.

## III. IMPLEMENTATION AND RESULTS

NS3 implemented this protocol. We considered the dissemination of a network topology composed of 100 nodes and 25 distinct data variables. The new protocol is discovered to withstand pollution attack situations, i.e. the intermediate nodes in the network receive and process only valid data packets. In addition, packets are immediately authenticated by using this one-time hash value functions which are generated and stored in the disseminated data packets.

### 4.1 SECURITY AND PERFORMANCE ANALYSIS

First, the security provided by this protocol is performed and analyzed. Session key agreement-encryption and decryp -tion session keys are used.

This key is also generated and used locally, but it is not exchanged in the network. Lightweight which is simple yet does good mathematical operations and the encryptions techniques are used hence improves performance in nodes. Below charts gives between comparison graph on the number of data messages disseminated in each protocol namely DiDrip, and the newly proposed protocol. Network coding has reduced the total number of message packets.

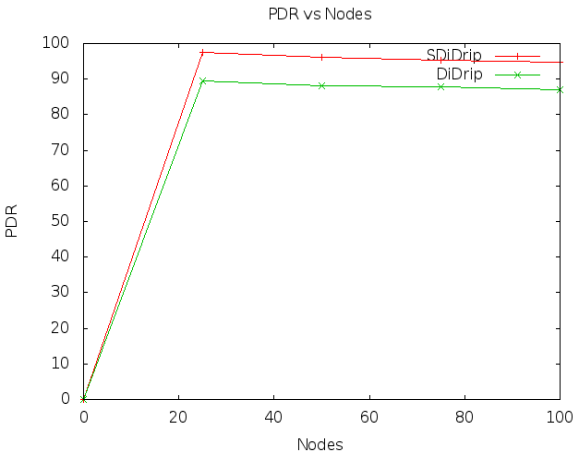


**Fig .2. Packet Delivery Ratio**

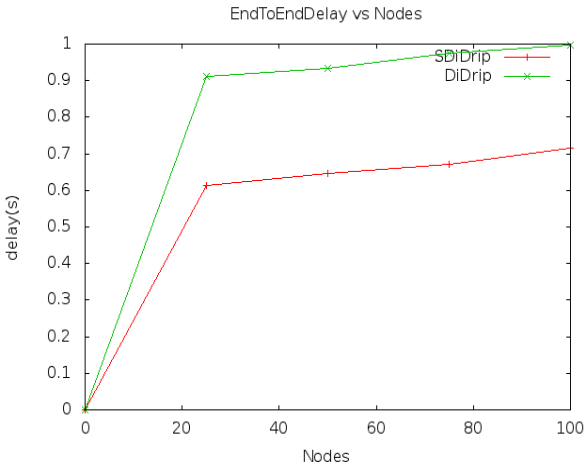


**Fig .3. End to End delay**



Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

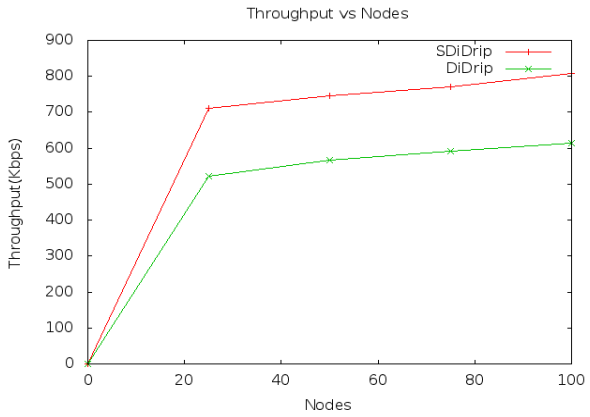


**Fig .4. Throughput**

## IV. CONCLUSION

In this article sec-didrip protocol is proposed which is a secure data discovery and dissemination protocol for the wireless sensor networks (WSN) that can be used specifically for limited configuration parameters and variables to accomplish secure and fast data dissemination. This method collaborates the concepts of network coding and hashing the data using simple cryptographic techniques to disseminate data. The advantages of this type of protocol are resistant and rigid against pollution attacks and that the dissemination of data achieves instant authentication. To encrypt and send information between nodes session keys are used and there is no need for the network to transfer the session keys. Also, to calculate keys for data encryption, only easy mathematical operations are used, so not much of the nodes resource use. An attacker's node compromise may be a problem in this protocol. It will be addressed as part of the work of the future.

## REFERENCES

1. Daojing He, Sammy Chan, Shaohua Tang and Mohsen Guizani, "Secure Data Discovery and Dissemination based on Hash Tree for Wireless Sensor Networks", IEEE transactions on wireless communications, Vol. 12, No. 9, September 2013.
2. P. Levis, N. Patel, D. Culler and S. Shenker, "Trickle: a self-regulating algorithm for code maintenance and propagation in wireless sensor networks", in Proc. 2004 NSDI, pp. 15-28.
3. G. Tolle and D. Culler, "Design of an application cooperative management system for wireless sensor networks," in Proc. EWSN, pp. 121–132, 2005.
4. Lin, K., Levis, P.: "Data discovery and dissemination with dip." In: Proceedings of the 2008 International Conference on Information Processing in Sensor Networks (IPSN 2008), Washington, DC, USA, IEEE Computer Society (2008) 433-444.

## AUTHORS PROFILE

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

**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 with 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.