ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Performance Analysis of Different Security Based Protocols for Wireless Sensor Network

Anagha A. Chaphadkar[1], Dr.Achala M. Deshmukh[2]

PG Student, Dept. of Digital Systems (Electronics), SCOE, Pune, India[1]

Professor, Dept. of E&TC, SCOE, Pune, India[2]

ABSTRACT: The different security techniques for novel data detection and broadcasting for wireless sensor networks which can be utilized to accomplish secure and quick data broadcasting particularly for small configuration parameters and variables. The significant applications, advantages and drawbacks of each algorithm can be discussed to obtain better protocols. Each of these techniques integrates the ideas of network coding and simple cryptographic techniques so as to broadcast data with at most security. Comparative analysis of all security techniques are provided to choose the best protocol against pollution attacks and Denial of Service attack. Best techniques are utilized to accomplishes immediate validation of data been scattered. Also simple mathematical operations are used to calculate keys for encryption of data so not much of resource usage at the nodes. All together it aims to provide simple yet secure and fast data scattering techniques for usage in wireless sensor networks.

KEYWORDS: DiDrip, DHV, DIP, Hash Key, SDD, SeDrip, WSN.

I. INTRODUCTION

WSN is one of the growing events in communication field. Because of networked collections of nodes, obtaining valuable information about the physical world becomes easy. WSN are utilized as a part of numerous applications like remote control and monitoring, construction safety systems, environmental monitoring, health care management, disaster management, surveillance operations, smart homes, habitat monitoring, indoor sensor networks, seismic monitoring of buildings and so on. WSN is made of different sensor nodes which can be utilized for monitoring and analysis purposes. The sensor nodes gather a data from a base station which is its prime location and then it can pass further by them. Gatewayis a medium which can be used by WSN to communicates with LAN or WAN. It permitsdevices tostore the information and which can be processed later. A sensor node is comprised of some basic components as shown in fig. (1): a circuit for interfacing with other sensor nodes, a micro controller, a radio transceiver, and a battery for power supply. The sensor node additionally hassome components such as a location finding system, a power generator and a mobilizerwhich are application dependent. A sensor node has another most important component that is power unit [4]. This power unit must possess following properties:

(i) consume extremely low power
(ii) operate in high volumetric densities
(iii) have low production cost and be dispensable
(iv) be adaptive to the environment

DOI: 10.15680/IJIRCCE.2017. 0504294

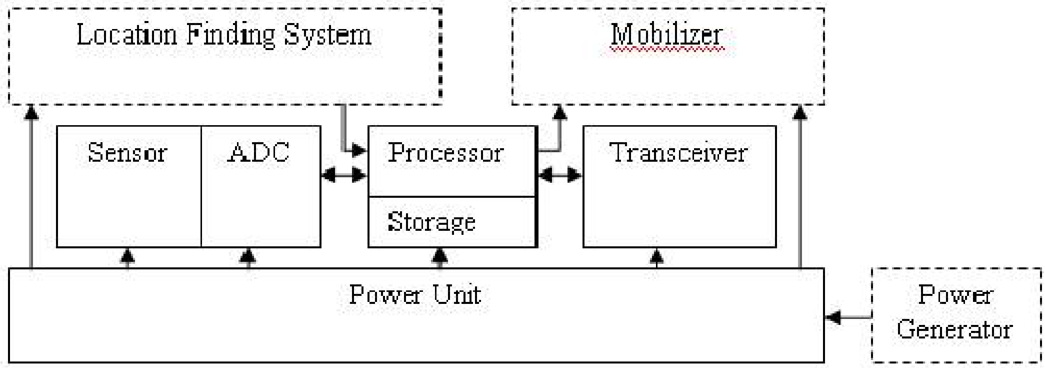

Figure 1: Components of Sensor nodes.

The topology utilized can be a star, ring, grid network or multi-hop wireless mesh network. WSN is utilized as a part of remote and hostile environments for data gathering which is essential application. Hence it is a major challenge to produce cheap sensor nodes. They must be designed carefully by considering all the different constraints of the environment.

II. LITERATURE REVIEW

To avoid the sending of data separately to each receiver, several multicast routing protocols have been proposed and established, typically in the IP layer. Although, each sensor network should have ability to available a human manager to quickly determine whether an established network is functioning or not.SNMS was presented for wireless sensor networks which provide an examination system to enable rapid, user-initiated acquisition of network health and performance data. It also allows a logging system to enable recording and retrieval of system-generated events. SNMS is simple and have negligible effect on memory and network activity, yet open and adaptable [3].The DIPwas proposedfor wireless networks that scale linearly with the number of data items. For T things, DIP can recognize new items with O (log (T)) packets while keeping up an O (1) detection latency [4].
Trickle was a code propagation mechanism, but it could be used to broadcast any data. One could change propagation scope by adding predicates to summaries, limiting the set of motes that consider them[5].A reliable distribution protocol for broadcasting a large data from multiple source nodes to many other nodes over a multihop wireless network was described in [5]. The propagation dynamics are characterized using a real-world deployment and simulation. A simple model is developed and used to identify different factors which limit the overall bandwidth of any multihop communication protocol [6].Dissemination protocols reliably deliver data to every node in a network using (key, version) tuples on top of some variant of the Trickle algorithm. A node detects a neighbor needs an update by observing that the neighbor has a lower version number for a data item (key) is the key characteristic [4]. Dissemination protocols such as XNP, Deluge, Sprinkler and MNP enables complete system reprogramming. Drip allowsdirectors to adjust configuration parameters and send RPC commands [7].Reprogrammingdepends on changes over some parameters of sensor node is accomplished through wireless communication using reprogrammable devices [8].The SCU system was designed forsecure reprogramming in a completelydecentralized fashion. The systemdistributes the new software using SYNAPSE++ asthe underlying protocol for data distribution [9].
Due to a vast disparity between sizes of programs and parameters, the design considerations of their dissemination protocols are different [10]. As a result, Code dissemination and data discovery and dissemination, thesetwo types ofprotocolsare developed [11].All existing protocols for code distributionfollow the centralized approach in which, data items can be broadcastedonly by the base station[2], [9]. It introduces the single point of failure. In that case distribution is not possible when the base station is not functioning or when the connection between the base station and a node is broken. Hence, code dissemination is carried out by authorized network users in a distributed manneris better approach [11].The security issues in data discovery and dissemination protocol of WSNs was investigated and point out that the lack of authentication of the disseminated data introduces a vulnerability to the update of random data

in WSNs. Then a secure, lightweight, and Denial-of-Service (DoS)-resistant data discovery and dissemination protocol named SeDrip was developed forWSNs, which is a secure extension of Drip [10].

A secure and distributed code dissemination protocol named Di-Code was proposed in [12].The salient feature of this Di-Code protocolis ability to resist denial of service attack.DiDrip satisfies the security requirements of thenetwork. Thepossible security technique can be applied to provethe authenticity and integrity of the distributeddata in DiDrip.In practice, the efficiency of DiDripcan be demonstrated by implementing it in an experimental WSN withresource-limited sensor nodes [13].DiDrip is based on shuffling, substitution and shifting to depict a security scheme for WSN which is energy efficient as well as difficult to crack [14].To disseminate the data between the nodes among the wireless sensor network four phases are used in DiDrip where it contains the main three mechanisms [15].

III. SEVERAL SECURITY TECHNIQUES AND THEIR COMPARISON

A. TESLA AND EMSS:

TESLA and EMSS are two important techniques for secure lossy multicast streams. TESLA is especially appropriate to give the source verification properties to the MESP header, or for the ALC protocol proposed by the RMT. TESLA offers sender confirmation, strong loss robustness, high scalability and minimal overhead, at the cost of loose initial time synchronization between the sender and the receivers and somewhat delayed verification. EMSS gives no rejection of origin, high loss resistance and low overhead, at the cost of somewhat delayed confirmation. The principle thought of TESLA is to have the sender append to every packets a MAC computed utilizing a key k known to itself only. The recipient buffers the received packet without having the capacity to verify it. If the packet is received too late then it is disposed of. After a short period, the sender releases key and the receiver can verify the packets [1].

Drawbacks in TESLA:

1. Buffering packets at the collector side may defer delivering the data to the application, may cause capacity issues, and furthermore produces vulnerability to denial-of-service.
2. Multiple keys have different exposure delay times results in larger overhead
3. Multiple senders need to perform time synchronization separately with every recipient.

B. SECURE TOPOLOGY DISCOVERY ALGORITHM :

Prevention from eaves dropping while discovering the routes can be done by providing a secret key to all sensor nodes and all the route information messages are encoded. The base station is relatively strong, and has the requisite processor speed, memory and energy to support the cryptographic and routing requirements of the sensor network.In the family of sensor routing protocols, every sensor node communicates either directly or indirectly with a base station. In turn the base station coordinates and aggregates information from each sensor. Accordingly, the base station will need to verify the authenticity of the sensor, the integrity of the communication and determine that it is not a repetition of an earlier communication. In this security protocol each sensorshares a unique 64 bit keywith the base station. The protocol provides for a multi-hop structure where the range of a base station is extended.

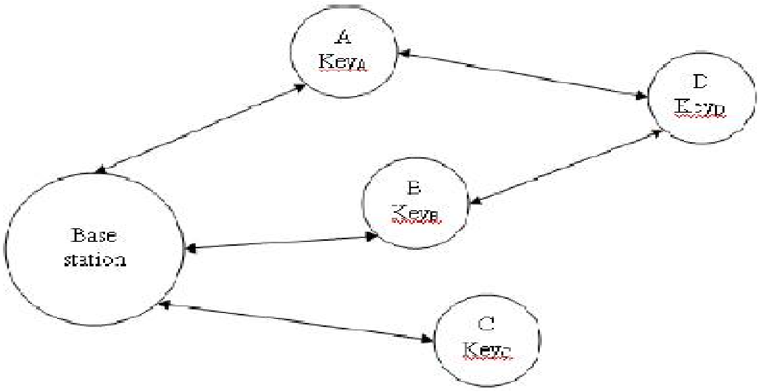

Figure 2: Example Network Topology

Figure 2 depicts an example of such a sensor network topology.The base station is located with the unique ID and similar encryption key of each node in the micro sensor network. Likewise, eachnode is located with the unique key that it shares with the base station and its clock is synchronized with the base station's clock [6].

C. DHV PROTOCOL:

DHV has two main phases that are detection and identification. In detection, each node broadcasts a hash of all its versions called a SUMMARY message. A node compares received hash got from its neighbor to its own hash. If there is difference, at least one code item with different version number is present. In identification, the horizontal search and vertical search steps are carried out to identify which versions are different. In horizontal search, anode broadcasts a HSUM message and compares received checksum from a neighbor, to its own checksum to identify which bitindices differ and proceeds to the next step. Similarly In vertical search,the node broadcasts a VBIT message. Itbroadcasts a bitslice of index 0 if the bit indicesare similar, but the hashes differ and increases the bit index to find the different locations until the hashes are the same.After identifying which (key, version)tuples differ, the nodebroadcasts these (key, version)tuples in a VECTOR message.Thena node compares received VECTOR message toits own (key, version)tuple to decide who has the newerversion. A node with anewer version broadcasts its DATA to nodes with an olderversion [8].The DHV protocol maintains the code stabilityin WSN. It helps to reducenetwork reprogramming latency and preserve energy consumptionin communication.

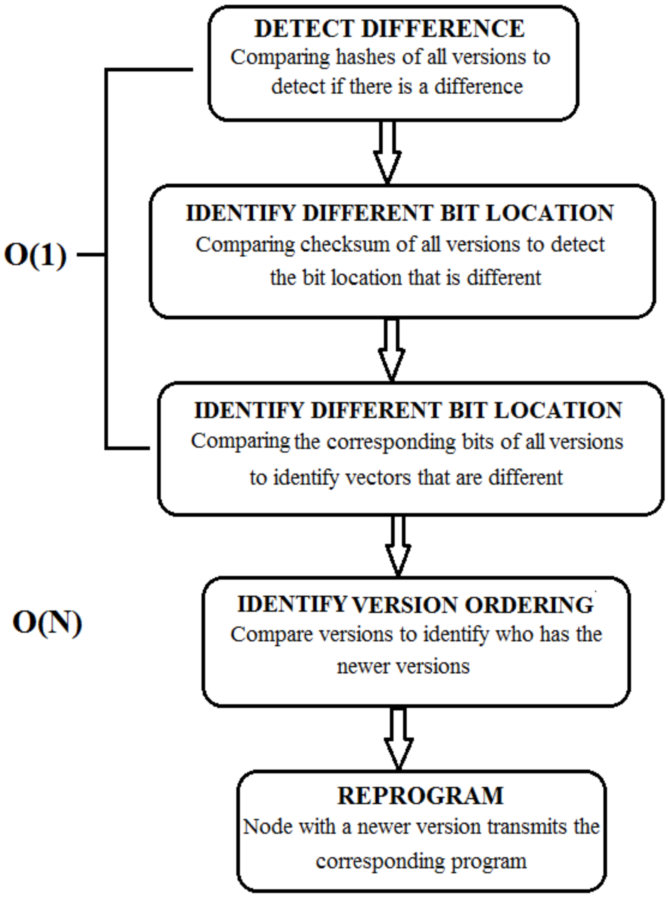
DETECT DIFFERENCE
Comparing hashes of all versions to detect if there is a difference
O(1)
IDENTIFY DIFFERENT BIT LOCATION
Comparing checksum of all versions to detect the bit location that is different
IDENTIFY DIFFERENT BIT LOCATION
Comparing the corresponding bits of all versions to identify vectors that are different
O(N)
IDENTIFY VERSION ORDERING
Compare versions to identify who has the newer versions
REPROGRAM
Node with a newer version transmits the corresponding program

Figure 3: DHV main components

Advantages of DHV:

1. It is able to reduce the total number of messages significantly.
2. Performance is better than DIP protocol.

Disadvantage of DHV:

1. It requires data consistency.

D. Secure Code Update Systems:

SCU system integrates into the confidentiality, protection against the dissemination of corrupted images and against Denial of Service (DoS) attacks [9]. Every security component has been streamlined representing the memory requirements of the chosen sensor platform and the collaborations with SYNAPSE++'s dissemination protocol. In the following way all the previously mentioned requirements are accomplished by SCU system.

Code Image Confidentiality: When the length of the data being encoded is bigger than the block size of the utilized encryption schedule, block ciphers must be combined with a supposed "operation mode". The CC2420 radio chip just executes the encryption capacity of AES-128. Therefore, OFB, CFB and CTR are the main possible operation modes and, among them, OFB is utilized as a part of SCU system because of its great execution.

Bogus Code Image Protection: Code image can be protected by signing the entire code image with a digital signature scheme. Sensor nodes accept a new code image only if its signature is valid, performing a bogus code image attack requires a forgery on the employed signature scheme. The success probability of such a forgery is negligible, when a proper digital signature scheme is utilized. However this approach permits identifying any corruption happening because of channel errors or malicious activities, it is not extremely productive. To guarantee all security property, a code image is validated at the BS before its dissemination.

DoS Protection: Fake messages may contain invalid data during a secure reprogramming event, that will be distinguished by the confirmation check but that will anyway force the receiver to perform long and energy expensive operations. Vaccinating a node from these attacks requires methods to recognize messages sent by trusted nodes and forged messages sent by malicious ones. These strategies combine packet-level verification with an appropriate set of counters called "nonces” to ensure the freshness of received messages. The CC2420 radio chip gives basic functionalities and offers answer for give protection against DoS attacks.

Advantages of SCU System:

It provides a full range of security mechanisms for WSNs.

Disadvantages of SCU System:

A small impact on the performance, while stick to the hardware limitations of sensor nodes.

E. DiCode Protocol:

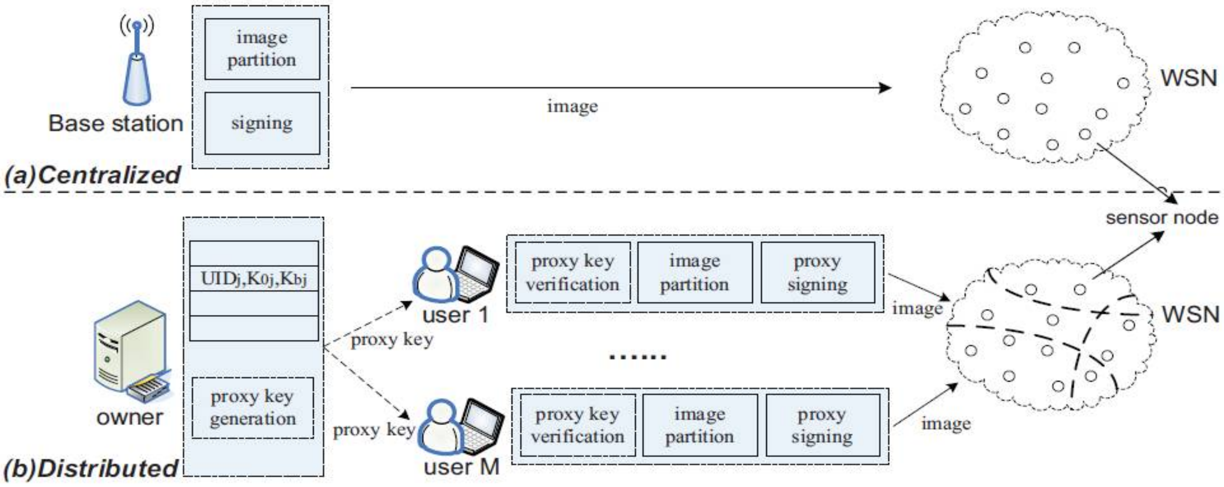

Figure 4: A system overview of (a) centralized and (b) distributed reprogramming approaches.

Code dissemination is the process of reprogramming of proper commands or updating of codes to sensor nodes after a WSN is located. Code dissemination is an important operation function of WSNsdue to the need of removing bugs and adding new functionalities.As a WSN is usually located in hostile environments; an enemy may put to use the code dissemination mechanism to introduce various attacks. Thus, secure code dissemination is a major concern.Since the design of Deluge did not take security into consideration, there have been several extensions to Deluge to provide security protection for code dissemination [9]. All previous code dissemination protocols [2], [9] are based on the centralized approach which assumes the existence of a base station and only the base station has the authority to reprogram sensor nodes.As shown in Fig. 5(a), A WSN broadcasts the signed code imagewhen it wants to broadcast a new code image and every sensor node accepts code images only signed by base station. Unfortunately it introduces a single point of failure and a very attractive attack target. A distributed approach can be employed for secure code dissemination in WSNs. The advantage of it is that the multiple authorizednetwork users can simultaneously and directly update code images on different nodes without involving the base station.Dicode protocol can be proposed by considering prevention to DoS attacks and stronger security techniques.PSW is introduced into the design of DiCode. This technique has two kinds of users, an original signer and proxy signers. The basic DiCode Protocol contains three phases: System initialization, User preprocessing and Sensor node verification. DiCode uses a digital signature technique for the verification of the program image. This signature is vulnerable to DoS attacks. Message specific puzzle and the improved message specific puzzle are described in the main protocol to prevent the attacks,which can complement the basic protocol of DiCode [11].
Advantages of DiCode:

1. It Ensures feasibility, security and efficiency for distributed code dissemination.
2. Avoid reprogramming conflict and support dynamic participation.
3. Different authorized users may be assigned different privileges of reprogramming sensor nodes.

Disadvantages of DiCode:

1. DiCodein WSN’s is time consumption at dissemination.

F. SeDrip Protocol:
Several data discovery and dissemination protocols [8], [4], [3] have been proposed. Among them, Drip [3], DIP [4] and DHV [8] are famous and added in TinyOS distributions. However, all existing protocolsonly address reliable data

transmission, but provide nosecurity mechanismand also assume benign environments[3]. Among the existing protocols, Drip organizes an independent trickle for each data item. In use, each data item contains a unique key to identify which variable it will update and a value to indicate its freshness. However, in hostile environments, data discovery and dissemination would face both external and insider attacks. To make these protocols secure, SeDrip protocol has been implemented with the advanced security issues.SeDripprotocol is a secure extension of Drip. SeDrip is based on a signed Merkle hash tree.Therefore the base station of a WSN needs to sign only the root of this tree. Hence to achieve DoS-attack flexibility and allow immediate verification of any received packets can be easier. SeDripis comprises of system initialization, packet pre-processing, and packet verification phases. To avoid frequent public key operations and achieve strong robustness against various malicious attacks SeDripintegrates ECC public key algorithm and Merkle hash tree algorithm. SeDrip protocol assumesthe base station as trustworthy and has unlimited computational power compared with sensor nodes. SeDrip uses a digital signature to bootstrap the authentication of each round of disseminated data. By immerse the WSN with a large number of illegal signature packets; an enemy can impose a DoS attack to the nodes. To resist this attack and to further improve the security and efficiency of SeDrip, the message specific puzzle approach [11] can be directly applied in SeDrip. Hence without first solving a message specific puzzle, the enemy cannot produce any forged packet which triggers a node to carry out the signature verification function.

Advantages of SeDrip:

1. Reliable data discovery and dissemination in WSNs.
2. Provides secure, lightweight and DoS-resistant data discovery and dissemination in WSNs.

G. SDD Protocol:

All previously proposed protocols [8], [4], [3] believe that the operating environment of the WSN is trustworthy and has no enemy attacks. However, in reality, adversaries exist and impose threats to the normal operation of WSNs [10]. This issue has only been addressed recently by [10] which identifies the security vulnerabilities of Drip and proposes an effective solution [11].SDD is carried in a distributed manner instead all existing protocols follow the centralized approach. SDDconsistsof four phases, system initialization, user joining, packetpreprocessing and packet verification.

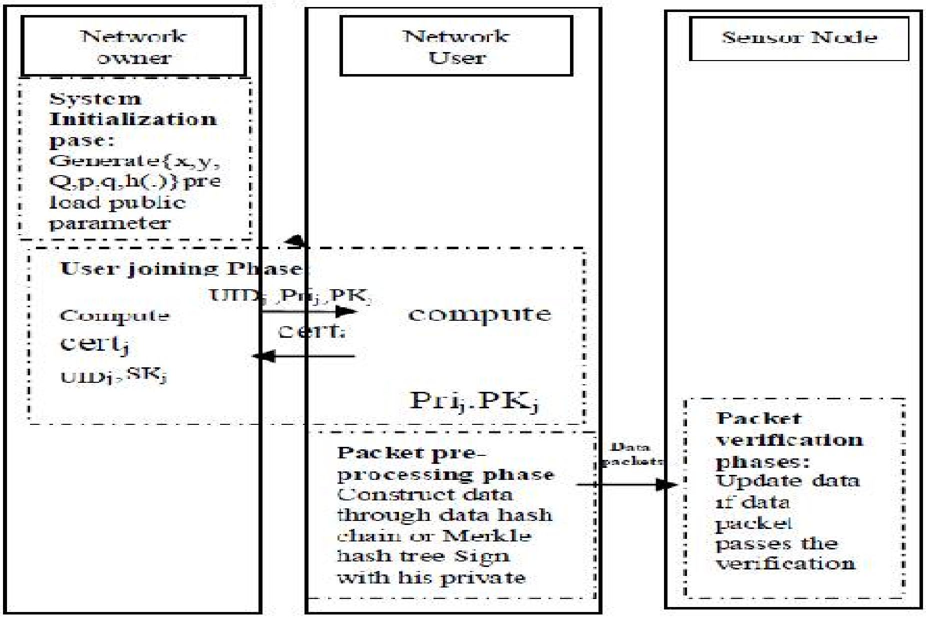
Network owner
Network User
Sensor Node
System Initialization pase: Generate{x,y, Q,p,q,h(.)} pre load public parameter
User joining Phase
UIDj ,Prij ,PKj
Compute certj
UIDj ,SKj
compute
certj
Prij .PKj
Packet pre-processing phase Construct data through data hash chain or Merkle hash tree Sign with his private
Data packets
Packet verification phases: Update data if data packet passes the verification

Figure 5: Information Process Flow in SDD

Advantages of SDD:

1. Allows network owners and users to disseminate data into WSN without relying on the base station.
2. It satisfies the security requirements such as authenticity and integrity of the disseminated data.

H. DiDrip Protocol:

Distributed data discovery and broadcasting is a growingly significant matter in WSNs, particularly in the setting of shared sensor networks, where detecting/communication frameworks from multiple owners and users will be shared by applications from multiple users. Distributed operation by networks owners and users with various benefits will be a critical issue, for which effective solutions are as yet absent. Secure and distributed data discovery and dissemination protocol (DiDrip) consists of four phases, system initialization, user joining, packet pre-processing and packet verification [3]. The data processing flow of DiDrip is outlined in Fig.5. The security vulnerabilities in data discovery and dissemination when utilized as a part of WSNs are recognized in DiDrip protocol, which have not been described in past research. Likewise, because of the open nature of wireless channels, messages can be effectively captured.

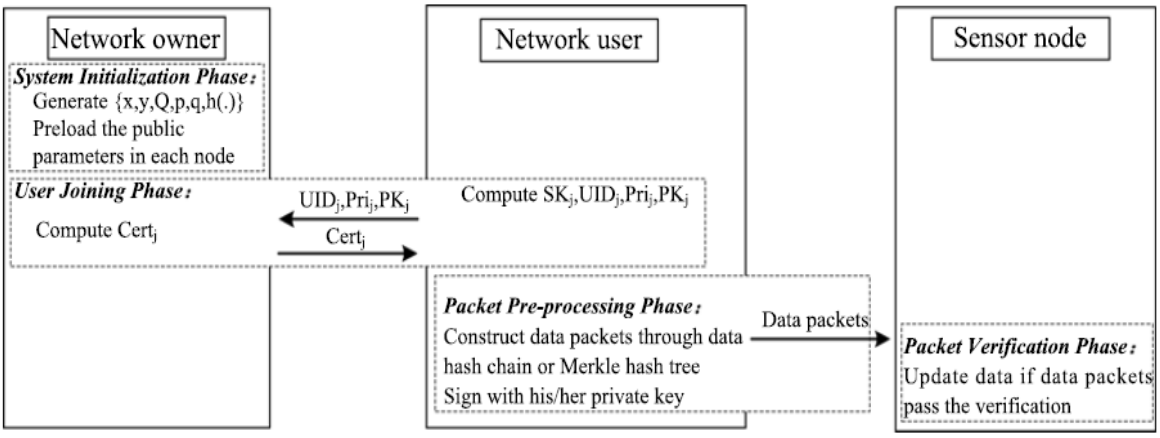
Network owner
System Initialization Phase:
Generate {x,y,Q,p,q,h(.)}
Preload the public parameters in each node
User Joining Phase:
Compute Cert$_j$
Network user
UID$_j$,Pri$_j$,PK$_j$
Cert$_j$
Compute SK$_j$,UID$_j$,Pri$_j$,PK$_j$
Packet Pre-processing Phase:
Construct data packets through data hash chain or Merkle hash tree
Sign with his/her private key
Data packets
Sensor node
Packet Verification Phase:
Update data if data packets pass the verification

Figure 6:Information Process Flow in DiDrip

Advantages of DiDrip:

1. Emergent context of shared sensor networks.
2. User can send data directly to the sensor nodes without using the base station.
3. Provides more security for data
4. Increases packet delivery ratio

IV. CONCLUSION

This paper proposes various security techniques for wireless sensor networks which can be used to achieve secure and fast data dissemination especially for small configuration parameters and variables. These techniques combine the concepts of network coding and simple cryptographic techniques so as to disseminate data. The comparative analysis of security and authenticity of different techniques can be given to find out best protocol for secure data discovery and dissemination. Also only simple mathematical operations are used to calculate keys for encryption and decryption of data so not much of resource usage at the nodes. Additionally various algorithms are added in the basic technique to extend the security and reliability of particular techniques. Every technique has some unique feature and hence it is far better than the previous one. All the relative advantages and improvements in each technique are described to make it more superior. All together this paper aims to provide a simple yet secure and fast data dissemination technique for usage in wireless sensor networks.

REFERENCES

[1] A. Perrig, R. Canetti, D. Song, and J. Tygar, "Efficient and secure source authentication for multicast," in Proc. Netw. Distrib. Syst. Security Symp., 2001.

[2] J. W. Hui and D. Culler, "The dynamic behaviour of a data dissemination protocol for network programming at scale," in Proc. 2nd Int. Conf. Embedded Netw. Sensor Syst., 2004, pp. 81–94.

[3] G. Tolle and D. Culler, "Design of an application-cooperative management system for wireless sensor networks," in Proc. Eur. Conf. Wireless Sensor Netw., 2005.

[4] K. Lin and P. Levis, "Data discovery and dissemination with DIP," in Proc. ACM/IEEE Int. Conf. Inf. Process. Sensor Netw., 2008, pp. 433–444.

[5] P. Levis, N. Patel, D. Culler, and S. Shenker, "Trickle: A self-regulatingalgorithm for code maintenance and propagation in wireless sensor networks," in Proc. 1st Conf. Symp. Netw. Syst. Design Implementation, 2004, pp. 15–28.

[6] M. Ismail and M. Y. Sanavullah, "Security topology in wireless sensor networks withRouting optimization" research scholar, electronics and communication, vinayaga mission university, 2008, pp.

[7] 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 Aquiladeployment," in Proc. IEEE Int. Conf. Inf. Process. Sensor Netw., 2009.

[8] T.Dang,N. Bulusu,W. Feng, and S. Park, "DHV:Acode consistency maintenance protocol for multi-hop wireless sensor networks," in Proc. 6th Eur. Conf. Wireless Sensor Netw., 2009, pp. 327–342.

[9] N. Bui et al., "An integrated system for secure code distribution inwireless sensor networks," in Proc. Percom'2010.

[10] D. He, S. Chan, S. Tang, and M. Guizani, "Secure data discovery and dissemination based on hash tree for wireless sensor networks," IEEE Trans. Wireless Commun., vol. 12, no. 9, pp. 4638–4646, Sep. 2013.

[11] D. He, C. Chen, S. Chan, and J. Bu, "DiCode: DoS-resistant anddistributed code dissemination in wireless sensor networks," IEEE Trans.Wireless Commun., vol. 11, no. 5, pp. 1946–1956, May 2012.

[12] S.Velmurugan and Dr. E. Logashanmugam, "Secure and Distributed Data in Wireless SensorNetwork," 2nd International Conference on Current Trends in Engineering and Technology, ICCTET'2014.

[13] D. He, S. Chan, H. Yang And B. Zhou, "Secure And Distributed Data Discovery And
Dissemination In WSN", IEEE Transactions On Parallel & Distributed S/m, Vol. 26, No. 4, April 2015

[14] Lekhana D N "A Novel Approach for Secure and Distributed Data in Cluster Based Wireless Sensor Network" (Volume-5, Issue-5) in Proc. IEEE Security Privacy, 2016, pp. 2278-9359

[15] "Distributed and Secure DiDrip Protocol for Data Discovery and Dissemination in WSNs", International Journal of Innovative Research in Science, Engineering and Technology (Vol. 5, Issue 4, April 2016)