 ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print)

The Recognition of Unauthorized User and Distribute Authenticity for Data in WSN

[1]Mamidi Jaya Ram, [2]KesavaraoSeerapu, [3]Dr. A. Chandra Sekhar
[1,2,3]Dept. of CSE, Avanthi Institute of Engineering and Technology, Vizianagaram, AP, India

Abstract
In Wireless Sensor Network, the security of data and secrecy of data is a dynamic perspective. Henceforth the data can't be hindered by the gatecrasher. For upgrading setup parameters and appropriating administration summons, data revelation and spread protocol for wireless sensor network is capable. Be that as it may, it has disadvantage is that, a few protocols were not planned with security. Thus, The DiDrip protocol i.e. to initiate with secure and dispersed data disclosure and spread protocol is proposed. The principle capacity of this protocol is for approved numerous network user. In this way, with the assistance of various security parameters the framework gives a high security to the wireless sensor network. Since the greater part of the WSN are setup in remote and threatening situations manual upgrading is not generally conceivable. So we have numerous spread protocols which help to reinvent the networks and make them steady with each other. Customary protocols like Drip, Deluge don't have any efforts to establish safety set up because of which fake code redesigns can be made by aggressors. Such a large number of secure data spread protocols have been acquainted with time with be utilized as a part of WSN.

Keywords
Dissemination, Multi Owner-Multi User Policy, Authentication, Data Integrity, Security, Wireless Sensor Network

I. Introduction
Wireless Sensor Network is a Network comprising of a gathering of sensor networks used to screen corporal and natural circumstance. Data Discovery and spread protocols are utilized for effectively upgrading parameters, old little projects put away in sensor networks after the wireless sensor network is conveyed. Numerous data revelation and disclosure and protocols [3-6] have been proposed for WSNs to be specific DHV, DIP, Drip. The proposed protocols accept that the WSN's working framework is dependable. In any case, as a general rule this is unimaginable in light of the fact that enemies exist and the dangers are forced to influence the ordinary operation of WSNs [7-9]. The existing data disclosure and scattering protocols are more over in light of brought together approach [3-7]. It means data must be dispersed by base station. The brought together approach experiences single purpose of disappointment. This implies when the association between the base station and hub is broken or when the base station is not working [2] data spread is unrealistic. The brought together approach is wasteful and nonscalable. Some WSNs don't have base station by any stretch of the imagination. The WSN is worked of "networks" – from a couple to a few hundreds or even thousands, where every hub is associated with one (or some of the time a few) sensors. Each such sensor network hub has regularly a few sections: A radio handset with an inward reception apparatus or association with an outer recieving wire, a microcontroller, an electronic circuit for interfacing with the sensors and aenergy source, typically a battery or an implanted type of energy reaping. A sensor hub may fluctuate in size from that of a shoebox down to the measure of a grain of clean, albeit working "bits" of honest to goodness minuscule measurements have yet to be made. The cost of sensor networks is likewise factor, going from a couple to several dollars, contingent upon the many-sided quality of the individual sensor networks. Size and cost imperatives on sensor networks bring about comparing limitations on assets, for example, energy, memory, computational speed and correspondences transmission capacity. In this paper chiefly comprises of two methodologies initial one is unified and the second ne is circulated in incorporated approach data things must be dispersed by the base station. The disservice of brought together approach is there might be odds of torment the single purpose of disappointment as dispersal is outlandish when the base station is not works legitimately or when the association between the base station and hub is broken. Remotely the unified approach is inefficacious, poise, and powerless against security assaults that can be propelled anyplace along the correspondence way [4]. Much more terrible case some WSNs don't have any base station. For instance, the WSNs observing human trafficking in a nation is outskirt or a WSNs conveyed in a remote territory to screen illicit or taboo remove development, a base station can turns into an alluring focus to be assaulted. In such a network, data flow is ideal to be completed by the proprietor or approved network users in a conveyed way. Besides, an appropriated data disclosure and scattering named DiDrip is exceptionally significant in wireless sensor networks. In shared sensor networks where detecting or correspondence frameworks from various proprietors will be shared by the applications from different users. These networks are possessed by different proprietors and utilized by different approved outsider users. Inspirations by the above perceptions, this paper has the accompanying fundamental commitments:

- The need of circulated data revelation and dispersal protocols is not totally new, but rather past work did not address this nee. We concentrate the useful necessities of such protocols, and set their plan targets. Likewise, we distinguish these security vulnerabilities in existing data disclosure and scattering protocols.
- Based on the outline targets, we propose DiDrip. It is the principal secure and dispersed data revelation and scattering protocol, which permits network proprietors and approved users to spread data things into the WSNs without depending on the base station. All the more ever our broad examination shows that DiDrip fulfills the security prerequisites of the protocols of its kind. Specifically, we apply the provable procedure to formally demonstrate the credibility and respectability of the dispersed data things in DiDrip.
- Also show the proficiency of DiDrip by and by executing it in an exploratory WSN with asset restricted sensor hub. This is likewise the principal execution of a protected and dispersed data disclosure and spread protocol.

II. Related Work
The principle goal of the creators [1] J. W. Hui is to break down a dependable data dispersal protocol for engendering huge data

objects from at least one source networks to numerous different networks over a multihop, wireless sensor network. Downpour works from earlier work in thickness mindful, pestilence support protocols. Utilizing both a genuine organization and reenactment, auhtors demonstrate that Deluge can dependably disperse data to all networks and portray its general execution. On Mica2-dab networks, Deluge can push almost 90 bytes/second, one-ninth the greatest transmission rate of the radio bolstered under TinyOS. Control messages are restricted to 18% of all transmissions. At scale, the protocol uncovered fascinating proliferation elements just alluded to by past spread work. A basic model is additionally inferred which depicts the breaking points of data engendering in wireless networks. At long last the rates got for scattering are naturally lower than that for single way engendering. It seems hard to altogether enhance the rate acquired by Deluge and i building up a tight lower bound as an open issue The new protocol DiCode is proposed by [2] D. He, C. Chen, S. Chan and J. Bu .Code dispersal in a wireless sensor network (WSN) is the way toward spreading another program picture or significant summons to sensor networks. As a WSN is typically sent in threatening situations, secure code scattering is and will keep on being a noteworthy concern. Most code scattering protocols depend on the unified approach in which just the base station has the power to start code spread. Be that as it may, it is attractive and once in a while important to disperse code pictures in a circulated way which permits numerous approved network users to at the same time and straightforwardly redesign code pictures on various networks without including the base station. Spurred by this thought, they built up a protected and conveyed code spread protocol named DiCode. A notable component of DiCode is its capacity to oppose disavowal of-administration assaults which have serious results on network accessibility. Facilitate, the security properties of Dicode protocol are exhibited by hypothetical examination. To confirm the effectiveness of the proposed approach by and by, the proposed component in a network of asset compelled sensor networks. DHV (Difference recognition Horizontal pursuit Vertical inquiry) [3] is a code consistency upkeep protocol given by Dang et al, a productive code consistency support protocol to guarantee that each hub in a network will in the end have a similar code. DHV depends on the basic perception that if two code variants are distinctive, their relating rendition numbers frequently vary in just a couple of minimum critical bits of their twofold representation. DHV permits networks to precisely choose and transmit just essential piece level data to distinguish a more up to date code form in the network. DHV can distinguish and recognize form contrasts in O(1) messages and idleness contrasted with the logarithmic size of current protocols. Plunge (Dissemination Protocol) is a data discovery and spread protocol proposed by [5] Lin et al. Earlier methodologies, for example, Trickle or SPIN, have overheads that scale straightly with the quantity of data things. For T things, DIP can distinguish new things with O(log(T)) parcels while keeping up an O(l) location inertness. To accomplish this execution in a wide range of network arrangements, DIP utilizes a half and half approach of randomized filtering and treebased coordinated pursuits. By powerfully selecting which of the two calculations to utilize, DIP beats both as far as transmissions and speed. Recreation and testbed tests demonstrate that DIP sends 20-60% less bundles than existing protocols and can be 200% quicker, while just requiring O(log(log(T))) extra state per data thing. The essential test of giving security works in WSNs is the constrained abilities of sensor networks as far as calculation, energy and capacity.

III. Security Vulnerabilities in Data Discovery and Dissemination

A. Review of Data Discovery and Dissemination The underlying algorithm of both DIP and Drip is Trickle. Initially, Trickle requires each node to periodically broadcast a summary of its stored data. When a node has received an older summary, it sends an update to that source. Once all nodes have consistent data, the broadcast interval is increased exponentially to save energy. However, if a node receives a new summary, it will broadcast this more quickly. In other words, Trickle can disseminate newly injected data very quickly. Among the existing protocols, Drip is the simplest one and it runs an independent instance of Trickle for each data item. In practice, each data item is identified by a unique key and its freshness is indicated by a version number. For example, for Drip, DIP and DHV, each data item is represented by a 3-tuple, where key is used to uniquely identify a data item, version indicates the freshness of the data item (the larger the version, the fresher the data), and data is the actual disseminated data (e.g., command, query or parameter). B. Security Vulnerabilities in Data Discovery and Dissemination An adversary can first place some intruder nodes in the network and then use them to alter the data being disseminated or forge a data item. This may result in some important parameters being erased or the entire network being rebooted with wrong data. For example, consider a new data item (key, version, data) being disseminated. When an intruder node receives this new data item, it can broadcast a malicious data item (key, version*, data*), where version* > version. If data* is set to 0, the parameter identified by key will be erased from all sensor nodes. Alternatively, if data* is different from data, all sensor nodes will update the parameter according to this forged data item. Note that the above attacks can also be launched if an adversary compromises some nodes and has access their key materials. In addition, since nodes executing Trickle are required to forward all new data items that it receives, an adversary can launch denial-of-service (DoS) attacks to sensor nodes by injecting a large amount of bogus data items. As a result, the processing and energy resources of nodes are expended to process and forward these bogus data items, rather than on the intended functions. Any data discovery and dissemination protocol based on Trickle or its variants is vulnerable to such a DoS attack.

IV. Distributed Trust and Provenance Models for WSN

A. Sensor Trust Analysis

WSNS are emerging technologies that have been widely used in many applications such as emergency response, healthcare monitoring, battlefield surveillance, habitat monitoring, traffic management, smart power grid [1], etc. The wireless and resource-constraint nature of a sensor network makes it an ideal medium for malicious attackers to intrude the system. Providing security is extremely important for the safe application of WSNs.

Various security mechanisms, e.g., cryptography, authentication, confidentiality, and message integrity, have been proposed to avoid security threats such as eavesdropping, message replay, and fabrication of messages. These approaches still suffer from many security vulnerabilities, such as node capture attacks and denial-of-service (DoS) attacks. The traditional security mechanisms can resist external attacks, but cannot solve internal attacks effectively which are caused by the captured nodes. To establish secure communications, we need to ensure that all communicating nodes are trusted. This highlights the fact that it is critical to establish

a trust model allowing a sensor node to infer the trustworthiness of another node.

Many researchers have developed trust models to build up trust relationships among sensor nodes [11]. For example, a distributed Reputation-based Framework for Sensor Networks (RFSN) is first proposed for WSNs. Two key building blocks of RFSN are Watchdog and Reputation System. Watchdog is responsible for monitoring communication behaviours of neighbour nodes. Reputation System is responsible for maintaining the reputation of a sensor node. The trust value is calculated based on the reputation value. In RFSN, only the direct trust is calculated while the recommendation trust is ignored. A Parameterized and Localized trUst management Scheme (PLUS). In PLUS, both personal reference and recommendation are used to build reasonable trust relationship among sensor nodes. Whenever a judge node receives a packet from suspect node, it always checks the integrity of the packet. If the integrity check fails, the trust value of suspect node will be decreased irrespective of whether it was really involved in malicious behaviours or not. Suspect node may get unfair penalty. Another similar trust evaluation algorithm named as Node Behavioural strategies banding belief theory of the Trust Evaluation algorithm (NBBTE) is proposed based on behaviour strategy banding D-S belief theory [9]. NBBTE algorithm first establishes various trust factors depending on the communication behaviours between two neighbour nodes. Then, it applies the fuzzy set theory to measure the direct trust values of sensor nodes. Finally, considering the recommendation of neighbour nodes, D-S evidence theory method is adopted to obtain integrated trust value instead of simple weighted-average one. To the best of our knowledge, NBBTE is the first proposed algorithm which establishes various trust factors depending on the communication behaviours to evaluate the trustworthiness of sensor nodes. Therefore, NBBTE is chosen as the comparing algorithm in this paper.

B. Provenance Verification Scheme

Sensor networks are used in numerous application domains, such as cyber physical infrastructure systems, environmental monitoring, power grids, etc. Data are produced at a large number of sensor node sources and processed in-network at intermediate hops on their way to a base station (BS) that performs decision-making. The diversity of data sources creates the need to assure the trustworthiness of data, such that only trustworthy information is considered in the decision process. Data provenance is an effective method to assess data trustworthiness, since it summarizes the history of ownership and the actions performed on the data. Recent research highlighted the key contribution of provenance in systems where the use of untrustworthy data may lead to catastrophic failures. Although provenance modelling, collection, and querying have been studied extensively for workflows and curate databases, provenance in sensor networks has not been properly addressed. We investigate the problem of secure and efficient provenance transmission and processing for sensor networks and we use provenance to detect packet loss attacks staged by malicious sensor nodes.

In a multi-hop sensor network, data provenance allows the BS to trace the source and forwarding path of an individual data packet. Provenance must be recorded for each packet, but important challenges arise due to the tight storage, energy and bandwidth constraints of sensor nodes. Therefore, it is necessary to devise a lightweight provenance solution with low overhead. Furthermore, sensors often operate in an untrusted environment, where they may be subject to attacks. It is necessary to address security requirements such as confidentiality, integrity and freshness of provenance. Our goal is to design a provenance encoding and decoding mechanism that satisfies such security and performance needs. We propose a provenance encoding strategy whereby each node on the path of a data packet securely embeds provenance information within a Bloom filter (BF) that is transmitted along with the data. Upon receiving the packet, the BS extracts and verifies the provenance information. We also devise an extension of the provenance encoding scheme that allows the BS to detect if a packet drop attack was staged by a malicious node.

As opposed to existing research that employs separate transmission channels for data and provenance, we only require a single channel for both. Furthermore, traditional provenance security solutions use intensively cryptography and digital signatures and they employ append-based data structures to store provenance, leading to prohibitive costs. In contrast, we use only fast message authentication code (MAC) schemes and Bloom filters, which are fixed-size data structures that compactly represent provenance. Bloom filters make efficient usage of bandwidth, and they yield low error rates in practice.

C. Issues on Sensor Node Security

Sensor data are streamed from multiple sources through intermediate processing nodes. Data provenance is applied to evaluate the trustworthiness of sensor data. Low energy and bandwidth consumption, efficient storage and secure transmission factors are considered in provenance management. Secure provenance verification scheme is used to authorize sensor data packets. In packet Bloom filters (iBF) are used to encode provenance. Provenance verification and reconstruction tasks are carried out under the base station. Secure provenance scheme is extended with functionality to detect packet drop attacks. Provenance collection algorithm and provenance verification algorithm are used in the data verification process. The following drawbacks are identified from the existing system. Multiple consecutive malicious sensor nodes based attacks are not handled. Packet lose detection accuracy is low. Node level trust factors are not considered. Time bounded provenance verification is not supported.

V. Attacks during Dissemination

External and internal attacks occur during dissemination. External attack is performed by attackers external to networks but the internal attacks are more dangerous one as attackers is already in the network.

A. Eavesdropping Attack

the eavesdropping attack is an external attack .It can be passive or active. In passive eaves dropping message is being listened from broadcast medium. In active eavesdropping, node enacts as valid node and grabs information. Encryption techniques are used to prevent this type of attack [9].

B. Replay Attack

A replay attack or playback attack is a kind of attack in which a valid data transfer is repeated or delayed by attackers. Packet signature, verification operations and Bloom filters are some techniques to prevent occurrence of replay Attacks.

C. Pollution Attack

This kind of attack is seen primarily during data dissemination in WSN. It can be used to pollute or flood the network with false data. Especially when network coding technique is used invalid network coded data is stored as intermediate nodes in a node path. To overcome this attack cryptographic technique like homomorphic hashing, identity certificates and signatures can be used [10].

D. Sybil Attack

In this type of attack a malicious node imitates other nodes or simply by claiming false identity. In data dissemination Sybil attack collects vital messages from the base station. So Sybil attacks must be dealt with as well. Many techniques have been proposed like identity certificates, methods based on Merkle hash tree [1].

E. Denial of Service Attack

Lack of proper authentication leads to valid packets being denied of their required status. Due to the characteristics of energy-sensitivity, dynamic nature of nodes and limited resources, sensor networks are very vulnerable to DoS attacks. Proper authentication schemes can be used in data dissemination to avoid this kind of attack. Se-Drip is one such protocol [2].

VI. Secured Data Distribution in WSN

The secure provenance verification scheme is enhanced to handle consecutive malicious node attacks. Efficient Distributed Trust Model (EDTM) is improved with security features. Integrated verification scheme is designed to authorize the node and data. Coordinated trust model is constructed with communication, energy, data and recommendation trust values.

The sensor network security system is designed to manage node and data verification operations. Anonymous data and malicious data forwarding operations are controlled by the system. Trust verification is performed to ensure network level security. The system divided into six major modules. They are Base Station, Provenance Management, Trust Assignment, Data Verification, Node Verification and Attack Handler. The base station is deployed to manage the wireless sensor network. Provenance management module handles the provenance release operations. Node level trust values are estimated under trust assignment module. Provenance verification is carried out under the data verification process. Node verification is performed with trust details.

Packet dropping attacks are managed under attack handler.

The base station manages the sensor nodes in WSN. Sensor nodes and their properties are maintained under the base station. Authentication and verification operations are carried out under base station. Data request operations are initiated from the base station. The base station releases the provenance for each node. Sensor data trust is ensured with data provenance. Provenance is encoded with in packet Bloom filters (iBF) data structures. Provenance graph is constructed with node information.

Reliability, utility, availability, risk and quality of services factors are considered in the trust assignment process, Trust assignment is performed with coordinated trust model, each node is assigned with four trust values, Communication, energy, data and recommendation trust values are used in the system. Secure provenance verification scheme is adapted to carry out the data verification process, Provenance collection algorithm is used to identify the presence of a node in provenance graph, Provenance and its integrity are checked using the provenance verification algorithm, The provenance verification process is enhanced with time bounded model. Node verification is performed with Efficient Distributed Trust Model (EDTM). Trust values are used to verify the belief of a node. EDTM uses one hop trust model and multi hop trust model for the node verification process. Security features are integrated with the EDTM scheme.

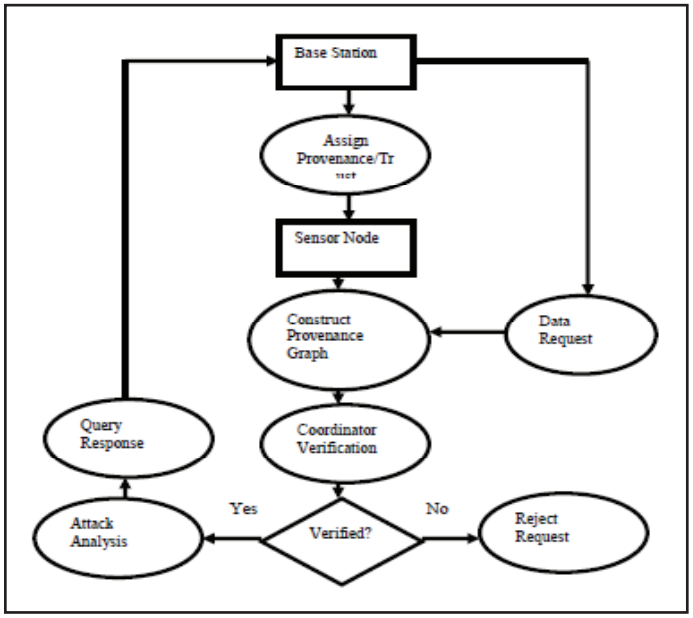

Fig. 1: Secured Data Distribution Scheme

Packet dropping attacks and malicious data forwarding attacks are detected under attack handler. Acknowledgement with sequence number is verified to identify the packet drop attacks. The system also detects multiple consecutive malicious sensor nodes based attacks. Path changes are suggested.

VII. Proposed System

DiDrip consists of four phases, system initialization, user joining, and packet pre-processing and packet verification. For our basic protocol, in system initialization phase, the network owner creates its public and private keys, and then loads the public parameters on each node before the network deployment. In user joining phase, a user gets the dissemination privilege through registering to the network owner. In packet pre-processing phase, if a user enters to the network and wants to dissemination some data items, he/she will need to construct the data dissemination packets and then send them to the nodes. In packet verification phase, a node verifies each received packet. If the result is positive, it updates the data according to the received packet. Based on the design objectives, they propose DiDrip. It is the first distributed data discovery and dissemination protocol, which allows network owners and authorized users to disseminate data items into WSNs without relying on the base station. Moreover, our extensive analysis demonstrates that DiDrip satisfies the security requirements of the protocols of its kind. In particular, they apply the provable security technique to formally prove the authenticity and integrity of the disseminated data items in DiDrip.In this paper, in order to enhance the security and mutual authentication to each and every node, a trust based model is followed. According to this method, the rating of each node is maintained at each node level. The ratings of a node will be done through the ratio of packet forwarded by

packets received. The node selection is based on the ratings. The nodes which are having high-rating are considered as trusted one and data packets are routed through them.

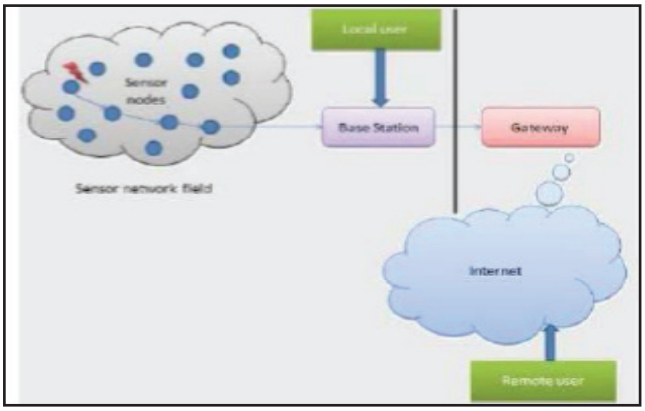

Fig. 2: Proposed System Architecture

VIII. Results

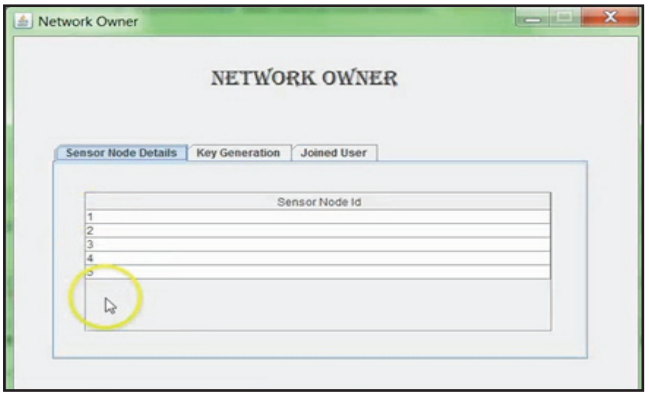

Fig. 3:

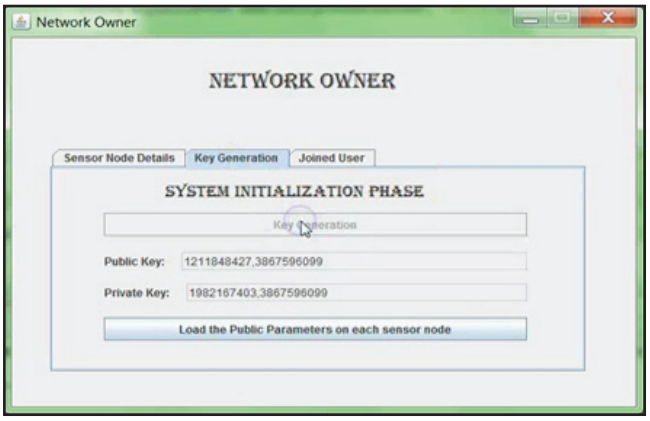

Fig. 4:

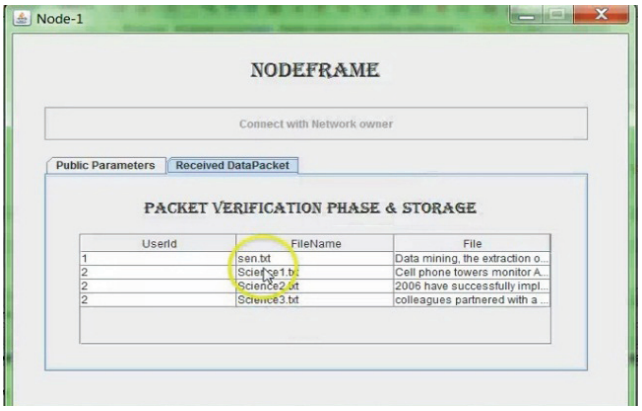

Fig. 5:

Fig. 6:

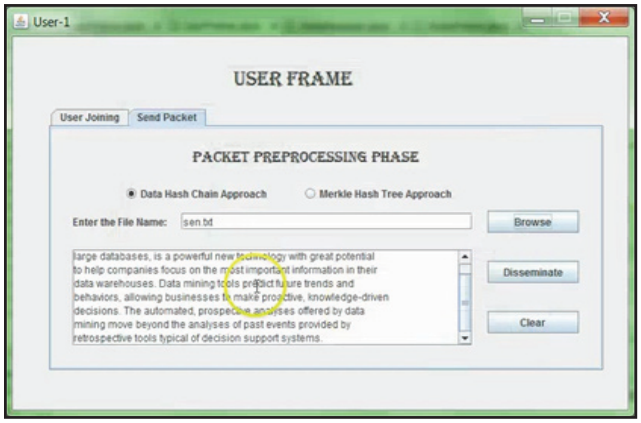

Fig. 7:

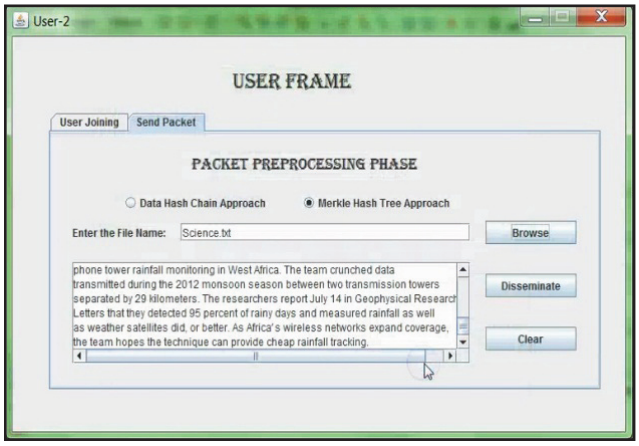

Fig. 8

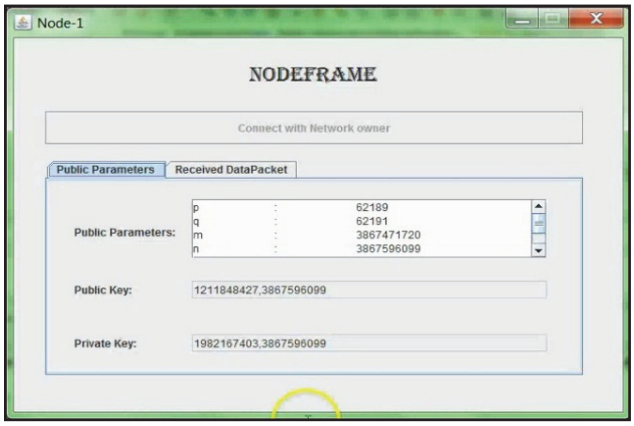

Fig. 9:

IX. Conclusion

Since there is no fixed topology in these networks, one of the greatest challenges is routing data from its source to the destination. Generally these routing protocols are motivated from two fields; WSNs and MANET. WSN routing protocols provide the required functionality but cannot handle the high frequency of topology changes. MANET routing protocols can deal with mobility in the network but they are designed for two way communication, which in sensor networks is often not required. But in case of mobile Wireless sensor, MANET protocols are used for WSN. AODV, DSR, DSDV, AOMDV protocols are preferred as they are able to work in mobile environments, whereas WSN protocols often aren't suitable. After all the above protocol, it is concluded that DSR is Suitable for mobile wireless sensor network. As parameter which are fit for Data dissemination like Packet delivery ratio, packet drop ratio, end to end delay, total received packet and command packet are better in case of DSR.

References

[1] Daojing He, Sammy Chan, Yan Zhang, HaomiaoYang, "Lightweight and Confidential Data Discovery and Dissemination for Wireless Body Area Networks", IEEE Journal of Biomedical and Health Informatics, Vol. 18, No. 2, pp. 440-448, March 2014.

[2] Mohammad A. Matin,"Wireless Sensor Networks: Technology and Protocols", Published by InTech, Croatia, 2012.

[3] Jisha Mary Jose, Jomina John,"Data dissemination protocols in wireless sensor networks-a survey", IJARCCE, March 2014.

[4] Daojing He, Sammy Chan, Shaohua Tang, 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.

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

[6] Nildo dos Santos Ribeiro Junior, Marcos A. M. Vieira1, Luiz F. M. Vieira, Om Gnawali,"CodeDrip: Data Dissemination Protocol with Network Coding for Wireless Sensor Networks", In Proceedings of the 11th European conference on Wireless sensor networks (EWSN 2014), Feb. 2014.

[7] T. Ho, D. Lun,"Network Coding: An Introduction", Cambridge University Press, 2008.

[8] 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) pp. 433-444.

[9] P. Levis, N. Patel, D. Culler, S. Shenker,"Trickle: A self-regulating algorithm for code maintenance and propagation in wireless sensor networks", In Proc. 2004 NSDI, pp. 15-28.

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

MAMIDI JAYA RAM Pursuing M.Tech (CSE) From AVANTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY Vizianagaram, A.P, India. His area of interest includes Cloud Computing and Network Security.

Mr. KesavaraoSeerapu, M.Tech (CSE), Assistant Professor, Department of CSE Avanthi Institute of Engineering &Technology, Vizianagaram, AP, INDIA. He is an M.Tech post graduate in Computer Science &Engg. from JNTU Kakinada. He attended several seminars and workshops. His goal in his life is to do Ph.D and research on advanced topics and serve for the mother country.

He believes in the wordings of **"Swami Vivekananda":**
"ARISE, AWAKE AND STOP NOT TILL THE GOAL IS REACHED".

Dr. A.Chandra Sekhar, Professor & HOD of Department of Computer Science And Engineering Avanthi Institute of Engineering &Technology, Vizianagaram, AP, Affiliated to JNTU Kakinada. He attended several seminars and workshops. He published several International Papers which shows his zeal towards research.

He believes in the wordings of **"Albert Einstein":**
"THE TRUE SIGN OF INTELLIGENCE IS NOT KNOWLEDGE BUT IMAGINATION".