ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Protected and Dispersed Data Detection and Diffusion in Wireless Sensor Networks

S.Md Ismail, M.Tech
Associate Professor,
Department of CSE,
Al-Habeeb College of Engineering &Technology, Chevella, Hyderabad.

Mr.Mohd Anwar Ali, M.Tech
Associate Professor & HOD,
Department of CSE,
Al-Habeeb College of Engineering &Technology, Chevella, Hyderabad.

Rendla Gopal Reddy
Post Graduate Student,
Department of CSE,
Al-Habeeb College of Engineering &Technology, Chevella, Hyderabad.

ABSTRACT:

Wireless sensor networks (WSN) are basically distributed networks or a collection of sensor nodes which collect information which are used to analyses physical or environmental conditions. WSNs are usually setup in remote and hostile areas and work in extreme conditions. Applications of WSN include habitat monitoring, industrial applications, battlefield surveillance and smart homes etc. Most of them require regular updating of software in sensor nodes through the wireless channel for efficient management and working. So it is necessary to spread data through the wireless medium after the nodes are deployed. This is known as data dissemination or network reprogramming. A good data dissemination protocol must be fast, secure, reliable and energy efficient. To achieve these we can make use of network coding techniques which reduces the number of retransmissions due to any packet drops. But network coding increases the chance of various kinds of network attacks. Also to avoid spreading of malicious code in the network, each sensor node has to authenticate its received code before propagating it further. So here a novel dissemination protocol is introduced based on simple cryptographic techniques which prevents pollution and DoS attacks and at the same time achieves fastness using the technique of network coding.

Keywords:

Wireless sensor network; dissemination; reprogramming; network coding; security; pollution attack.

1. INTRODUCTION:

Wireless Sensor Networks (WSN) is one of the major milestones in the field of communication. These networked collections of nodes take us a step closer to obtaining valuable information about the physical world. WSN are used popularly in many 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 etc. In computer science and communication wireless sensor networks entertain lot of research today. A WSN is made of sensor nodes used for monitoring and analysis purposes as shown in Fig 1. These sensor nodes pass the information that they collect to a prime location called a base station. In most systems, a WSN communicates with a LAN or WAN through a gateway like medium.

The gateway is actually a bridge between the WSN and the various other networks [2]. This allows data to be stored by devices and which can be taken up for processing later. Each sensor node or mote has several parts: a circuit for interfacing with other sensor nodes, a micro controller, a radio transceiver, and a battery for power supply. The topology used can be either a star, ring, grid network or multi-hop wireless mesh network.WSN is used primarily in remote and hostile environments for information collection. 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 in consideration after a wireless sensor network (WSN) is deployed, there is usually a need to update buggy/old small programs or parameters stored in the sensor nodes. This can be achieved by the so-called data discovery and dissemination protocol, which facilitates a source to inject small programs, commands, queries, and configuration parameters to sensor nodes. Note that it is different from the code dissemination protocols (also referred to as data dissemination or reprogramming protocols)

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

which distribute large binaries to reprogram the whole network of sensors. For example, efficiently disseminating a binary file of tens of kilobytes requires a code dissemination protocol while disseminating several 2-byte configuration parameters requires data discovery and dissemination protocol. Considering the sensor nodes could be distributed in a harsh environment, remotely disseminating such small data to the sensor nodes through the wireless channel is a more preferred and practical approach than manual intervention. In the literature, several data discovery and dissemination protocols have been proposed for WSNs. Among them, DHV, DIP and Drip are regarded as the state-of-the-art protocols and have been included in the Tinos distributions. All proposed protocols assume that the operating environment of the WSN is trustworthy and has no adversary. However, in reality, adversaries exist and impose threats to the normal operation of WSNs.

Objective of the Project:

In Wireless Sensor Network, the security of data and confidentiality of data is an important aspect. Hence the data cannot be interrupted by the intruder. For updating configuration parameters and distributing management commands, data discovery and dissemination protocol for wireless sensor network is responsible. But, it has drawback is that, some protocols were not designed with security. For this reason, The DiDrip protocol i.e. first secure and distributed data discovery and dissemination protocol is proposed. The main function of this protocol is for authorized multiple network user. So, with the help of different security parameters the system provides a high security to the wireless sensor network. Energy efficient new algorithm is also used because it is difficult to crack.

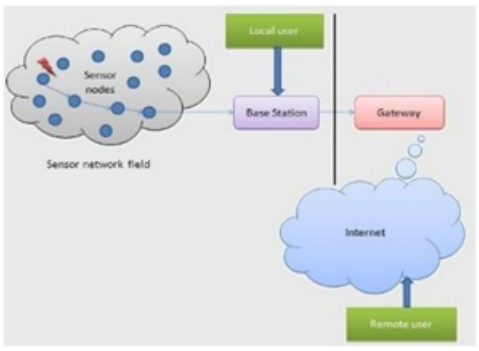


Fig1: An example wireless sensor network

Wireless sensor networks must be operated for long duration of time and usually don't get any human administration or intervention in between. Evolving conditions and environments can also; cause hanges in application features, which hence lead to the need to change the network behavior by introducing new code or software. But the remote nature of WSN is a disadvantage here. It will require the propagation of new code updates over the wireless medium i.e. over the air as manual updating of such networks will not be possible. This process is known as dissemination or network reprogramming. Onemajor challenge is proper and complete dissemination of information to all sensor nodes in the network.

This is difficult since the number of nodes in the network can be huge and the environment is always dynamic, thus the basic topology keeps changing constantly. Secondly the information to be disseminated may be produced at a single node, such as the prime source i.e. the base station, or at thesensor nodes themselves. Thirdly data must be disseminated in a secure way or else adversaries can track out critical data. Also there is a possibility of attackers sending bogus data into the network which must not be received by the sensor nodes as they can cause different attacks like pollution attacks, denial of service attacks and so on. So dissemination of code or program data in wireless sensor networks is an area to be worked in deeply and new techniques need to be introduced to achieve tradeoffs between energy and speed in dissemination. The aim of this work is to develop a novel secure and fast data dissemination protocol for use in wireless sensor networks.

This work concentrates on developing a dissemination protocol for dissemination of small data. Linear network coding is a technique used to achieve fastness and energy efficiency during dissemination It is a technique that combines packets in the network; increasing the throughput, decreasing energy consumption, and reducing the number of messages transmitted. In traditional systems dropped packets are recovered using retransmissions. But in network coding we can combine packets using mathematical operations and then disseminate so that recovery of lost packets can be achieved without retransmission.

2. RELATED WORKS:

Data dissemination in wireless sensor networks is a critical and vital task. It is based on the concept of traditional communication system, where we have a sender and receiver.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The scenario is basically a sender sending out some information, and receiver collecting the information sent, processing it and sending some information back. While in data dissemination, only half of this concept is applied. Some information is sent out and received at the destination, but no reply is given back. The sender sends out information, not to one node, but to many as in a broadcasting system.Dissemination is used to send code updates or program images to the sensor nodes periodically so as to perform reprogramming of the nodes. This over the air act is required since manual updating of sensor nodes deployed in remote environments is next to impossible in most of the cases. The main aim of a dissemination protocol in WSN is to ensure that all the sensor nodes have consistent data with them always. There are two kinds of dissemination in WSN:

•Code dissemination - to send program images which are generally bulky data. Usually they are divided into fixed sized pages and packets and then disseminated.
•Data discovery and dissemination - to disseminate small configuration parameters, variables, queries, commands etc in packets.

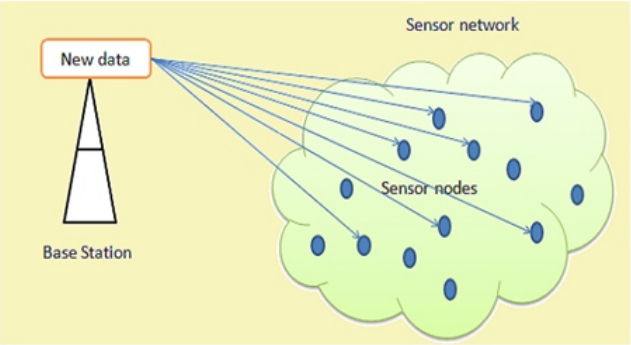


Fig2: Dissemination process in WSN

2.1 Small Value Dissemination:

This work concentrates on data discovery and dissemination protocols i.e. dissemination of small values like variables, parameters and so on gives a general idea about data dissemination. Traditional protocols available for this include Drip, DIP and DHV. The simplest of all dissemination protocols and is based on Trickle algorithm and establishes an independent trickle for each variable in the data. Every time an application wants to transmit a message, a new version number is generated and used. This will cause the protocol to reset the Trickle timer and thus disseminate the new value else the trickle timer interval is incremented.

DIP (Dissemination Protocol) is a data detection and dissemination protocol proposed by Lin et al. It is a protocol based on the Trickle algorithm. It works in two parts: determining whether there a difference in data stored at a node, and then determining which data is different. It is based on the concept of version number and key tulle for each data item. DIP calculates hashes that cover all version numbers of the data. Nodes that receive hashes same as their own know that they have consistent data with respect to their nearest neighbors. If a node gets a hash that differs from its own hash, it knows that a difference exists in the data.

DHV (Difference detection-Horizontal search-Vertical search) is a code consistency maintenance protocol given by Dang et al. It tries to keep codes on different nodes in a WSN consistent and up to date. Here also data items are represented as tuples (key, version). It is based on the observation that if two data items are different, they will only differ in a few least significant bits (LSB) of their version number rather than in all their bits. So only those bits need to be checked. For this steps followed are detection and identification.

There are many code dissemination protocols like Deluge as well. They are used to disseminate large code updates into the network. For this the code is often broken down into pages and then further into packets. Here we have seen some basic data discovery and dissemination protocols. They don't support any techniques which help to reduce packet retransmissions. Also none of these protocols provide security to the data disseminated.

2.2 Network Coding and Data Dissemination:

Network coding aims to replace the traditional store and forward technique used in networks; by better routing algorithms that will allow intermediate nodes to transform the moving data. Network coding has become popular due to its properties like robustness and better throughput. It helps to achieve fast data dissemination as it reduces the number of retransmissions that will be needed if there are packet losses. Many dissemination protocols have been developed using the concept of network coding. The advantages of network coding based dissemination protocols are that they achieve energy savings and communication efficiency, especially during increased packet loss or network density. So network coding based protocols can be profitable for reprogramming of WSNs.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

However we face a potential problem in hostile environments. An adversary may launch pollution attacks, in which a malicious node sends bad encoded packets that consist of bogus data, which leads to incorrect decoding of the original data upon retrieval. Here we use binary network coding i.e. the mathematical operation used is XOR to combine the contents of packets. Only two packet network coding is done here. Also here we focus on dissemination of small values like configuration parameters, variables, queries, commands etc whose size range from 2-4 bytes and thus is modification of the existing DRIP protocol.

3. ASSUMPTIONS AND THREAT MODEL

3.1 Assumptions:

Here assume that the source of the reprogramming variables the base station, is a secure location. Also each sensor node has a unique identification number. We assume that while each sensor node is resource limited, it has sufficient memory to store all the security mechanisms of the protocol.

3.2 Threat Model:

Here assume that the individual sensor-nodes are unprotected. An adversary may insert its own attacker nodes into the network, or it may capture other nodes. The adversary can attempt to launch pollution attacks to corrupt the data in the network and also to consume the limited resources on sensor nodes.

3.3 Existing System:

Data Discovery and dissemination protocols are used for easily updating parameters, old small programs stored in sensor nodes after the wireless sensor network is deployed. Many data discovery and discovery and dissemination protocols have been proposed for WSNs namely DHV, DIP, Drip. The proposed protocols assume that the WSN's operating system is trustworthy. But in reality this is impossible because adversaries exist and the threats are imposed to affect the normal operation of WSNs. The existing data discovery and dissemination protocols are more over based on centralized approach. It means data can only be disseminated by base station. The centralized approach suffers from single point of failure. This means that when the connection between the base station and node is broken or when the base station is not functioning data dissemination is not possible. The centralized approach is inefficient and non-scalable.

Disadvantages of Existing System:

1.In existing, more chances to attacks harm on network that means security is less.
2.When the connection between base station and node is broken, the data discovery and dissemination is impossible.

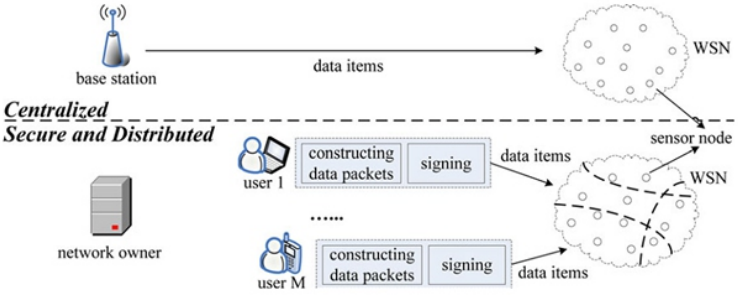
3.4 Proposed System:

This paper proposes the first secure and distributed data discovery and dissemination protocol named DiDrip. It allows the network owners to authorize multiple network users with different privileges to simultaneously and directly disseminate data items to the sensor nodes without relying on base station. DiDrip satisfies the security requirements of the protocols.

Advantages of Proposed System:

1.Improved security mechanisms.
2.Multiple authorized users allow to disseminate data items into wireless sensor networks without depends on base station.
3.WSNs are protected by Denial of Service (DoS) attacks.

SYSTEM ARCHITECTURE:



3.5 Packet Processing Phase:

Before disseminating data a node will generate a real time key using a key generation algorithm. This includes the generation of two unique random numbers R1_node and R 2_node. Key generation is done using Trivium-Multilinear Modular Hashing (MMH) as the MAC function and SHA1 as hashing function H(x). The steps are:

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

3.6 Packet Verification Phase:

To achieve immediate authentication of the received packet, the destination node will calculate the hash of R m stored in its memory and compare it with the value in the received packet. If they match, then the received packet is a valid node. Thus it will be acknowledged ACK by the destination. Otherwise a NACK (negative ack) is sent to the sender. Next we will have to ensure the integrity of the data. For this first the node checks the id in the received packet. If it is a valid node_id, then it will attempt to decrypt the data using the session key already generated and stored. Every node has an original data and combined data buffer. So the node will check whether it is an original data or combined data. If it is an original data it will be stored and disseminated after a trickle timer fire and if it is a combined data, the node will check whether it is possible to extract any other data from this newly received data using network coding. After that the data will be stored or disseminated out. So likewise all the data disseminated from the original source node will be distributed to all the nodes and a round of dissemination will be completed. This technique thus makes sure that only valid data is sent out and data is been sent out safely.

4.IMPLEMENTATION AND RESULTS:

This protocol has been implemented in TinyOS-2.1.2 simulator TOSSIM. We have considered a network topology consisting of 100 nodes and 25 different data variables are disseminated. The packet size in TinyOS is 29bytes. The sensor node considered for simulation here is micaz. Cryptographic support has been achieved using hashing algorithms like SHA-1 which generates a 160 bit hash value, MAC functions like Trivium Multilinear Modular Hashing (MMH), and symmetric encryption algorithms like AES which uses a 128 bit key. The new protocol is found to resist cases of pollution attacks i.e. only valid data packets are received and processed by the intermediate nodes in the network. Also immediate authentication of packets is achieved using the one time hash value generated and stored in the data packets disseminated.

4.1.Economic Feasibility:

A system can be developed technically and that will be used if installed must still be a good investment for the organization.

In the economical feasibility, the development cost in creating the system is evaluated against the ultimate benefit derived from the new systems. Financial benefits must equal or exceed the costs. The system is economically feasible. It does not require any addition hardware or software. Since the interface for this system is developed using the existing resources and technologies available at NIC, There is nominal expenditure and economical feasibility for certain.

4.2.Operational Feasibility :

Proposed projects are beneficial only if they can be turned out into information system. That will meet the organization's operating requirements. Operational feasibility aspects of the project are to be taken as an important part of the project implementation. This system is targeted to be in accordance with the above-mentioned issues. Beforehand, the management issues and user requirements have been taken into consideration. So there is no question of resistance from the users that can undermine the possible application benefits. The well-planned design would ensure the optimal utilization of the computer resources and would help in the improvement of performance status.

4.2. TECHNICAL FEASIBILITY:

Earlier no system existed to cater to the needs of 'Secure Infrastructure Implementation System'. The current system developed is technically feasible. It is a web based user interface for audit workflow at NIC-CSD. Thus it provides an easy access to .the users. The database's purpose is to create, establish and maintain a workflow among various entities in order to facilitate all concerned users in their various capacities or roles. Permission to the users would be granted based on the roles specified. Therefore, it provides the technical guarantee of accuracy, reliability and security.

5.SECURITY AND PERFORMANCE ANALYSIS:

First we perform and analyze the security offered by this protocol.

•Resistance to pollution attacks- Attackers can't pollute the network with bogus data since data transfer done is always verified using cryptographic techniques.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

•Resistance to Denial-of-Service attacks- Immediate authentication of packets is done at each destination, so bogus packets can be discarded and only valid packets pass through.
•Session key agreement- Session keys are used for encryption and decryption. Also this key is locally generated and used, hence not exchanged in the network.
•Real time key generation- No-pre stored keys in nodes; they are calculated at time of data transfer only.
•Light-weight- Only simple yet good mathematical operations and encryptions techniques are used hence no much resource usage in nodes.

An effective technique to securely synchronize the data and source node with the sink node in the network, without transmission of synchronization control message separately. Here we focus on ensuring that each node gets synchronized with sink nodes also event ordering on sink node can be achieved and nodes along the data delivery path such that event reports is generated by the sink are ordered properly. With our scheme we are able to achieve our main goal of synchronizing events at the sink and the data delivery with quickness, accuracy, security.

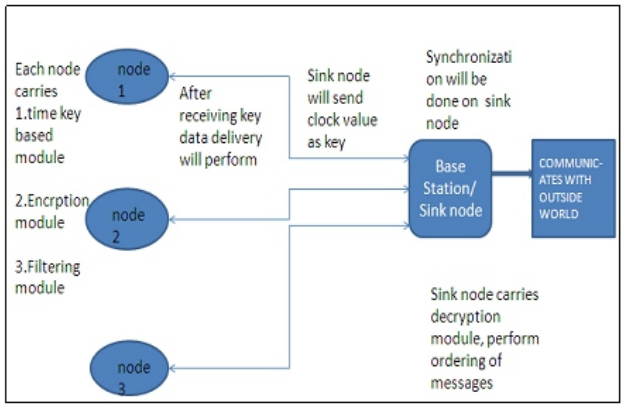


Fig: Scheme of Work

Different nodes of wireless sensor network firstly communicate with base station or sink node through wireless medium using RF module, then base station sends local time as key to the nodes with the help of this key synchronization can be achieved on sink node again for secure communication RC6 encryption algorithm used for secure data delivery to the sink node ,sink node carries decryption algorithm through which original data can be obtained ,event ordering also takes place on sink node. Sink node able to send data to the outside world or other network. It will reduce energy consumption as wireless sensor network have one of the major issue of energy consumption, also with no requirement of synchronization control message it provides quickness with less delay in data delivery. Also RC6 is lightweight algorithm and good enough to provide security.

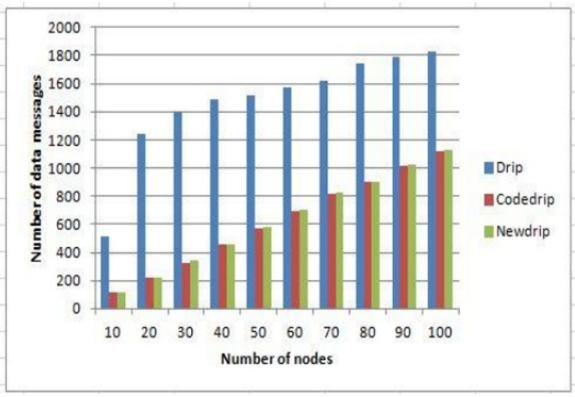


Fig: Comparison of data messages disseminated

6.LITERATURE SURVEY:

The Dynamic Behavior of a Data Dissemination Protocol for Network Programming at Scale To support network programming, we present Deluge, a reliable data dissemination protocol for propagating large data objects from one or more source nodes to many other nodes over a multihop, wireless sensor network. Deluge builds from prior work in density-aware, epidemic maintenance protocols. Using both a real-world deployment and simulation, we show that Deluge can reliably disseminate data to all nodes and characterize its overall performance. On Mica2- dot nodes, Deluge can push nearly 90 bytes/second, oneninth the maximum transmission rate of the radio supported under TinyOS. Control messages are limited to 18% of all transmissions. At scale, the protocol exposes interesting propagation dynamics only hinted at by previous dissemination work. A simple model is also derived which describes the limits of data propagation in wireless networks. Finally, we argue that the rates obtained for dissemination are inherently lower than that for single path propagation. It appears very hard to significantly improve upon the rate obtained by Deluge and we identify establishing a tight lower bound as an open problem.

Seluge:

Secure and DoS-Resistant Code Dissemination in Wireless Sensor NetworksWireless sensor networks are considered ideal candidates for a wide range of applications, such as industry monitoring, data acquisition in hazardous environments, and military operations.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

It is desirable and sometimes necessary to reprogram sensor nodes through wireless links after deployment, due to, for example, the need of removing bugs and adding new functionalities. The process of propagating a new code image to the nodes in a wireless sensor network is referred to as code dissemination.

DHV:

A Code Consistency Maintenance Protocol for Multi-Hop Wireless Sensor Networks Ensuring that every sensor node has the same code version is challenging in dynamic, unreliable multi-hop sensor networks. When nodes have different code versions, the network may not behave as intended, wasting time and energy. We propose and evaluate DHV, an ef- ficient code consistency maintenance protocol to ensure that every node in a network will eventually have the same code. DHV is based on the simple observation that if two code versions are different, their corresponding version numbers often differ in only a few least significant bits of their binary representation. Design of an application-cooperative management system for wireless sensor networksThis paper argues for the usefulness of an application-cooperative interactive management system for wireless sensor networks, and presents SNMS, a Sensor Network Management System.

SNMS is designed to be simple and have minimal impact on memory and network traffic, while remaining open and flexible. The system is evaluated in light of issues derived from real deployment experiences.We have described SNMS, a simple and robust application-cooperative Sensor Network Management System. SNMS provides a core set of services to enable management: query-based health data collection and persistent event logging. These services occupy a minimal amount of RAM and code size, and can be rapidly integrated into TinyOS applications. To ensure that these services are usable for management and will continue to function in the event of application failure.

Data Discovery and Dissemination with DIP:

We present DIP, a data discovery and dissemination protocol for wireless networks. Prior approaches, such as Trickle or SPIN, have overheads that scale linearly with the number of data items. For T items, DIP can identify new items with O(log(T)) packets while maintaining a O(1) detection latency.

To achieve this performance in a wide spectrum of network configurations, DIP uses a hybrid approach of randomized scanning and tree-based directed searches. By dynamically selecting which of the two algorithms to use, DIP outperforms both in terms of transmissions and speed. Simulation and testbed experiments show that DIP sends 20-60% fewer packets than existing protocols and can be 200% faster, while only requiring O(log(log(T))) additional state per data item.Monitoring Heritage Buildings with Wireless Sensor Networks: The Torre Aquila DeploymentWireless sensor networks are untethered infrastructures that are easy to deploy and have limited visual impact—a key asset in monitoring heritage buildings of artistic interest. This paper describes one such system deployed in Torre Aquila, a medieval tower in Trento (Italy). Our contributions range from the hardware to the graphical front-end. Customized hardware deals efficiently with high-volume vibration data, and specially-designed sensors acquire the building's deformation. Dedicated software services provide: i) data collection, to efficiently reconcile the diverse data rates and reliability needs of heterogeneous sensors; ii) data dissemination, to spread configuration changes and enable remote tasking; iii) time synchronization, with low memory demands. Unlike most deployments, built directly on the operating system, our entire software layer sits atop our Teeny LIME middleware. Based on 4 months of operation, we show that our system is an effective tool for assessing the tower's stability, as it delivers data reliably.

Secure Data Dissemination Protocol in Wireless Sensor Networks Using XOR Network Coding Wireless sensor networks (WSN) are basically distributed networks or a collection of sensor nodes which collect information which are used to analyse physical or environmental conditions. WSNs are usually setup in remote and hostile areas and work in extreme conditions. Applications of WSN include habitat monitoring, industrial applications, battlefield surveillance, smart homes etc. Most of them require regular updating of software in sensor nodes through the wireless channel for efficient management and working. So it is necessary to spread data through the wireless medium after the nodes are deployed. This is known as data dissemination or network reprogramming. A good data dissemination protocol must be fast, secure, reliable and energy efficient. To achieve these we can make use of network coding techniques which reduces the number of retransmissions due to any packet drops. But network coding increases the chance of various kinds of network attacks.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Also to avoid spreading of malicious code in the network, each sensor node has to authenticate its received code before propagating it further. So here a novel dissemination protocol is introduced based on simple cryptographic techniques which prevents pollution and DoS attacks and at the same time achieves fastness using the technique of network coding.

7. CONCLUSION:

his paper proposes a novel data discovery and dissemination protocol for wireless sensor networks which can be used to achieve secure and fast data dissemination especially for small configuration parameters and variables. This technique combines the concepts of network coding and simple cryptographic techniques so as to disseminate data. The advantages of this protocol are that it is resistant to pollution attacks, and achieves immediate authentication of data been disseminated. Session keys are used to encrypt and send data between nodes and there is no need of actual transfer of the session keys through the network. Also only 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 a simple yet secure and fast data dissemination protocol for usage in wireless sensor networks. Node compromise by an attacker can be an issue in this protocol. It will be dealt with as part of the future works shows that DiDrip is feasible in practice. We have also given a formal proof of the authenticity and integrity of the disseminated data items in DiDrip. Also, due to the open nature of wireless channels, messages can be easily intercepted.

8. References :

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

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

• 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.

•G. Tolle and D. Culler, "Design of an application-cooperative management system for wireless sensor networks," in Proc. Eur. Conf. Wireless Sensor Netw., 2005, pp. 121–132.

•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.

•M. Ceriotti, G. P. Picco, A. L. Murphy, S. Guna, M. Corra, M. Pozzi, D. Zonta, and P. Zanon, "Monitoring heritage buildings with wireless sensor networks: The Torre Aquila deployment," in Proc. IEEE Int. Conf. Inf. Process. Sensor Netw., 2009, pp. 277–288.

•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.

•M. Rahman, N. Nasser, and T. Taleb, "Pairing-based secure timing synchronization for heterogeneous sensor networks," in Proc. IEEE Global Telecommun. Conf., 2008, pp. 1–5.

•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. 1st Conf. Symp. Netw. Syst. Design Implementation, 2004, pp. 15–28.