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

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 3, March 2016**

# Mechanism of Secure and Distributed Data Discovery and Dissemination in Wireless Sensor Networks

Indermohan Singh Major [1,] Dr. R. S. Kawitkar[2]

PG Student, Department of ETC, Sinhgad College of Engineering, Vadgaon (BK), Pune, Savitribai Phule Pune University, Pune India

Prof. Department of ETC, Sinhgad College of Engineering, Vadgaon (BK), Pune, Savitribai Phule Pune University, Pune India

**ABSTRACT:** Remote sensor frameworks (WSN) are in a general sense circled frameworks or a collection of sensor centers which accumulate information which are used to dismember physical or common conditions. WSNs are regularly setup in remote and undermining zones and work in awesome conditions. Uses of WSN consolidate living space checking, mechanical applications, battle zone observation, splendid homes et cetera. A vast segment of them require general overhauling of programming in sensor center points through the remote channel for viable organization and working. So it is essential to spread data through the remote medium after the centers are sent. This is known as data dispersing or framework rehashing. An OK data dispersing tradition must be speedy, secure, tried and true and essentialness capable. To fulfill these we can make usage of framework coding methodology which diminishes the amount of retransmissions as a result of any package drops. In any case, orchestrate coding manufactures the shot of various sorts of framework attacks. In like manner to keep away from spreading of malicious code in the framework, each sensor center point needs to affirm its got code before causing it further. So here a novel spread tradition is introduced in light of direct cryptographic methodologies which hinders defilement and DoS attacks and meanwhile achieves speed using the technique of framework coding.

**KEYWORDS:** Dissemination,network coding, pollution attack, reprogramming, security, wireless sensor network.

## I. INTRODUCTION

Remote Sensor Networks (WSN) is one of the noteworthy defining moments in the field of correspondence. These masterminded aggregations of centers make us a step closer to gaining vital information about the physical world. WSN are used noticeably as a part of various applications like remote control and checking, improvement security systems, natural watching, social protection organization, disaster organization, perception operations, splendid homes, living space watching, indoor sensor frameworks, seismic seeing of structures et cetera [1]. In programming designing and correspondence remote sensor frameworks fortify package of examination today. A WSN is made of sensor center points used for checking and examination purposes as showed up in Fig 1. These sensor center points pass the information that they accumulate to a prime region called a base station. In numerous systems, a WSN relates with a LAN or WAN through an entryway like medium. The section is truly an augmentation between the WSN and the distinctive frameworks [2]. This licenses data to be secured by contraptions and which can be taken up for get ready later. Each sensor center point or bit has a couple areas: a circuit for interfacing with other sensor center points, a scaled down scale controller, a radio handset, and a battery for power supply. The topology used can be either a star, ring, framework or multi-hop remote cross area framework. WSN is used essentially as a piece of remote and debilitating circumstances for information gathering. Along these lines it is an important test to convey disgraceful sensor centers. They ought to be made purposely by considering all the various goals of the earth in thought.

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

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 3, March 2016**

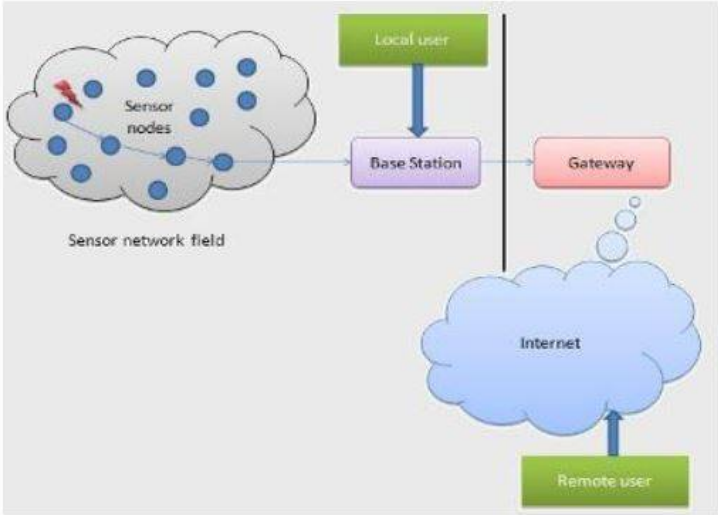


**Fig -1:** An example wireless sensor network

Remote sensor systems must be worked for long term of time and for the most part don't get any human organization or intercession in the middle of [3]. Advancing conditions and situations can likewise; cause changes in application highlights, which consequently prompt the need to change the system conduct by presenting new code or programming. Be that as it may, the remote way of WSN is a disservice here. It will require the proliferation of new code redesigns over the remote medium i.e. over the air as manual redesigning of such systems won't be conceivable. This procedure is known as spread or system reinventing. In any case, scattering acquires a considerable measure of difficulties [3]. One noteworthy test is legitimate and finish dispersal of data to all sensor hubs in the system. This is troublesome since the quantity of hubs in the system can be enormous and nature is constantly rapid, hence the essential topology continues evolving always. Furthermore the data to be scattered might be created at a solitary hub, for example, the prime source i.e. the base station, or at the sensor hubs themselves. Thirdly information must be scattered securely or else enemies can track out basic information. Additionally there is a probability of assailants sending sham information into the system which should not be gotten by the sensor hubs as they can bring about various assaults like contamination assaults, disavowal of administration assaults et cetera. So dispersal of code or program information in remote sensor systems is a zone to be worked in profoundly and new methods should be acquainted with accomplish tradeoffs in the middle of vitality and rate in spread. The point of this work is to build up a novel secure and quick information dispersal convention for use in remote sensor systems. This work focuses on adding to a dispersal convention for scattering of little information.

Straight system coding is a strategy used to accomplish speed and vitality effectiveness amid scattering [4]. It is a method that consolidates parcels in the system; expanding the throughput, diminishing vitality utilization, and decreasing the quantity of messages transmitted. In conventional frameworks dropped bundles are recouped utilizing retransmissions. In any case, in system coding we can join bundles utilizing scientific operations and after that disperse so that recuperation of lost parcels can be accomplished without retransmission. Be that as it may, system coding alongside its vitality productivity favorable circumstances gets a considerable measure of cerebral pains. It is profoundly inclined to assaults like contamination, foreswearing of-administration assaults and numerous others. So to manage these proposed framework utilizes straightforward however proficient cryptographic procedures for information scattering. This ensures we can accomplish straightforward yet secure information spread in remote sensor systems. Our work is sorted out as takes after. In the first place we concentrate on the need of information spread in remote sensor systems and some of its related works. Next the outline and usage which focuses on the spread of little values and variables is clarified. At that point we ponder the execution of the new convention through broad reproduction utilizing TinyOS lastly have the conclusion and references.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

## II. RELATED WORKS

Information dispersal in remote sensor systems is a basic and crucial undertaking. It depends on the idea of conventional correspondence framework, where we have a sender and beneficiary. The situation is fundamentally a sender conveying some data, and beneficiary gathering the data sent, preparing it and sending some data back. While in information scattering, just 50% of this idea is connected. Some data is conveyed and got at the destination; however no answer is given back. The sender conveys data, not to one hub, but rather to numerous as in a television framework. Dispersal is utilized to send code upgrades or program pictures to the sensor hubs intermittently in order to perform reconstructing of the hubs. This over the air demonstration is required since manual upgrading of sensor hubs conveyed in remote situations is alongside outlandish in a large portion of the cases. The principle point of a spread convention in WSN is to guarantee that all the sensor hubs have predictable information with them generally.There are two kinds of dissemination in WSN [5]:

1. Code dissemination - to send program images which are generally bulky data. Usually they are divided into fixed sized pages and packets and then disseminated.

2. Data discovery and dissemination - to disseminate small configuration parameters, variables, queries, commands etc in packets.

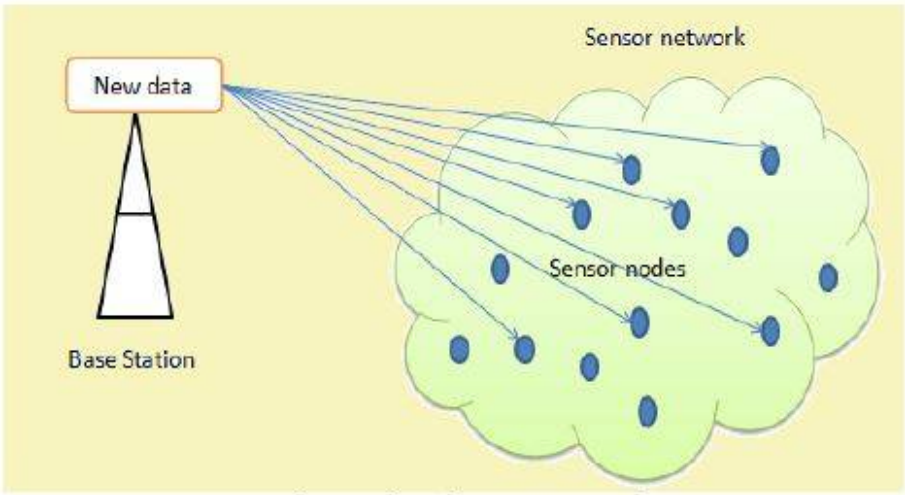


**Fig -2:** Dissemination process in WSN

### 1. Small Value Dissemination

This work focuses on information revelation and spread conventions i.e. dispersal of little values like variables, parameters etc. Figure 2 gives a general thought regarding information spread. Conventional conventions accessible for this incorporate Drip, DIP and DHV. They are all in view of Trickle calculation [6].
Trickle proposed by Tolle et. al [7] is the least difficult of all spread conventions and depends on Trickle calculation and sets up an autonomous stream for every variable in the information. Each time an application needs to transmit a message, another rendition number is created and utilized. This will bring about the convention to reset the Trickle clock and subsequently scatter the new esteem else the stream clock interim is augmented. Plunge (Dissemination Protocol) [8] is information identification and scattering convention proposed by Lin et al. It is a convention in view of the Trickle calculation. It works in two sections: figuring out if there a distinction in information put away at a hub, and after that figuring out which information is distinctive. It depends on the idea of form number and key tuple for every information thing. Plunge figures hashes that cover all form quantities of the information. Hubs that get hashes same as their own realize that they have steady information as for their closest neighbors. In the event that a hub gets a hash that

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

contrasts from its own particular hash, it realizes that a distinction exists in the information. DHV (Difference discovery Horizontal inquiry Vertical pursuit), [9] is a code consistency upkeep convention given by Dang et al. It tries to keep codes on various hubs in a WSN reliable and up and coming. Here likewise information things are spoken to as tuples (key, adaptation). It depends on the perception that if two information things are distinctive, they will just vary in a couple of slightest huge bits (LSB) of their adaptation number as opposed to in every one of their bits. So just those bits should be checked. For this strides took after are recognition and distinguishing proof. There are numerous code spread conventions like Deluge [10] also. They are utilized to disperse substantial code redesigns into the system. For this the code is regularly separated into pages and afterward encourage into bundles. Here we have seen some fundamental information revelation and scattering conventions. They don't support any methods which diminish bundle retransmissions. Additionally none of these conventions give security to the information spread.

### 2. Network Coding and Data Dissemination

System coding [4] plans to supplant the customary store and forward method utilized as a part of systems; by better directing calculations that will permit middle of the road hubs to change the moving information. System coding has ended up mainstream because of its properties like power and better throughput. It accomplishes quick information scattering as it decreases the quantity of retransmissions that will be required if there are bundle misfortunes. Numerous scattering conventions have been created utilizing the idea of system coding [4] [5].
The upsides of system coding based dispersal conventions are that they accomplish vitality investment funds and correspondence effectiveness, particularly amid expanded parcel misfortune or system thickness. So arrange coding based conventions can be gainful for reconstructing of WSNs. Nonetheless we confront a potential issue in antagonistic situations. A foe may dispatch contamination assaults, in which a malevolent hub sends terrible encoded parcels that comprise of sham information, which prompts inaccurate translating of the first information upon recovery.
Here we utilize twofold system coding i.e. the scientific operation utilized is XOR to consolidate the substance of bundles [4]. Just two bundle system coding is done here. Additionally here we concentrate on dispersal of little values like setup parameters, variables, questions, summons and so forth whose size extent from 2-4 bytes and along these lines is change of the current DRIP convention.

## III. ASSUMPTIONS AND THREAT MODEL

### 1 Assumption

Here expect that the wellspring of the reinventing variables, i.e., the base station, is a safe area. Additionally every sensor hub has a novel recognizable proof number. We expect that while every sensor hub is asset restricted, it has adequate memory to store all the security instruments of the convention.

### 2 Threat Model

Here expect that the individual sensor-hubs are unprotected. A foe may embed its own aggressor hubs into the system, or it might catch different hubs. The foe can endeavor to dispatch contamination assaults to degenerate the information in the system furthermore to expend the constrained assets on sensor hubs.

## IV. PROPOSED SYSTEM

In this protocol data dissemination is done in a secure and fast way by using the techniques of network coding and cryptography. Network coding reduces the number of retransmissions due to any packet losses happening in the network by combing and sending data. Also data disseminated is always sent as encrypted data. For this nodes first perform node to node authentication and establish session keys. Then the session key is used for encrypted transfer of data. This protocol ensures that the system is free of pollution [13] and Denial-of-Service attacks. The different phases of this protocol include:

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

**1 System Initialization Phase**
This phase is done before the WSN is deployed in the application field. In this phase the base station generates a master key Km and a unique random number Rm and stores them safely in each node. Also a list of all the valid node ids is maintained in each node.
**2 Packet Processing Phase**
In this phase the actual data dissemination occurs. 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 R2_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:

1. MAC[i] = R1_node XOR K[i] (1)

2. a[i] = node_id + MAC[i] (2)

3. h = MMH ( a[i] ) (3)

4. Key = H ( h XOR R2_node ) (4)

Where K[i] is the master key of the MAC function, node_id is the identifier of the corresponding node, XOR is the logical XOR operation. This real time key is broadcast by the node in a packet which will include the node_id and the key. The destination node who receives it will check the node_id with its list of valid nodes and ensure this packet is coming from a valid node. If yes that node will also generate a real time key using the same process as above and send back a reply packet to the sender node which will contain the node_id and the newly generated key. If this packet is also validated, then the two nodes are ready to generate a session key. The key is generated as:
Session key = Km XOR Ka XOR Kb (5)
Where Ka and Kb are keys generated at any two nodes A and B. Now this key is used for encrypting the data to be disseminated. The advantage of this scheme is that there is no need of actual exchange of the session key through the network. To encrypt the data we use symmetric encryption techniques preferably Advanced Encryption Standard (AES). So the data packet disseminated from a node will contain the data in encrypted form i.e.
Data = E (d)sk , where sk is the session key. (6)
Dissemination in wireless sensor networks works on the basis of Trickle algorithm [2]. It takes on the concept of gossiping. Whenever a new data is to be disseminated the trickle timer is reset to 0 and the data is broadcasted. When a node receives a new data it will store it. But if it receives a data which it already is aware of then it will increase the trickle timer interval and suppresses the duplicate incoming data.
To achieve immediate authentication of data packets a onetime hash of the initially generated random number is also calculated and included in each packet. The steps are:

1. Calculate Hash = H(Rm) (7)

2. Result = ADD(Hash) (8)

Where H( ) is SHA-1 and ADD( ) is basic addition operation. The result is included in the packets sent.
**3 Packet Verification Phase**
To achieve immediate authentication of the received packet, the destination node will calculate the hash of Rm 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.

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

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 3, March 2016**

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.

## V. IMPLEMENTATION AND RESULTS

This protocol has been implemented in TinyOS-2.1.2 simulator TOSSIM [7]. We have considered a network topology consisting of 100 nodes and 25 different data variables are disseminated. The packet size in TinyOS [8] 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 TriviumMultilinear 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.

## VI. SECURITY AND PERFORMANCE ANALYSIS

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

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

2. 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.

3. 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.

4. Real time key generation- No-pre stored keys in nodes; they are calculated at time of data transfer only.

5. Light-weight- Only simple yet good mathematical operations and encryptions techniques are used hence no much resource usage in nodes.

## VII. EXPERIMENTAL SETUP

We have assessed the execution of the proposed convention by reenactment utilizing Java [2]. We consider a rectangular district of zone 100£100m, in which the remote sensor hubs are conveyed in a specially appointed way. There is one BS to which all the sensor hubs in the system need to send their information bundles. The transmission scope of every hub is 20 m. We have contrasted the execution of proposed convention and SEEM [4]. Every reproduction trial was directed utilizing 10 distinctive system topologies, and every outcome was arrived at the midpoint of more than 10 keeps running of various system topologies. The execution of the planned convention is thought about under two conditions: ordinary conditions and conditions with half of pernicious hubs. The execution of the de-marked convention is measured by the quantity of sensor hubs hindered by an arrangement of traded off hubs in each round by expanding the quantity of bargained hubs in the net-Work. The accompanying key parameters are measured amid the reenactment run: Throughput. This is the rate of effectively gotten information bundles by BS. Control Overhead. Control overhead is characterized as the proportion of control parcels (Route Discovery, Route Discovery Reply, Neighbor Collection, Data dispersal Enquiry, and Data scattering Reply) to information transmissions.

System Lifetime. The lifetime of the system is characterized as the time at which the First hub disappointment happens, i.e., the time at which some hub's vitality re-serve is decreased to zero. The lifetime of a WSN is specifically connected to the vitality utilization of every hub. Hub Resilience. The hub resilience power after the assault happens on the

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

system. Figures 3, 4, 5 demonstrate the execution correlation of SEEM [2] and proposed convention when there is no at-tack on the system. From the Figures, we can watch that both SEEM and proposed plan have a high parcel conveyance proportion which increments as the quantity of hubs increments. Both SEEM and proposed plans select an ideal way from various decisions. The proposed plan picks the best way relying on R metric. 2. Likewise control overhead increments as the extent of the system increments. This is because of the way that both BS and sensor hubs need to control bundles to the entire system. At the point when the hubs thickness builds every hub has more neighbors and more control parcels are sent and got between neighbors. However the control overhead is less in the proposed plan than SEEM because of the way that proposed plan picks the best accessible way progressively by utilizing R metric. Additionally just the session key is required to validate the information to be sent to the separate hubs, while hub id is utilized for open key of every hub. Additionally organize lifetime increments than SEEM extensively. R metric in the proposed plan is versatile in nature and pick the best accessible way so that less vitality can be expended which directly affects the system lifetime. This is because of the way that all the past proposed plans utilize the same way for all interchanges between the source and BS. The immediate outcome of this is hubs on this specific way may drain vitality soon. Yet, in the proposed plan, the CH chooses another way with least estimation of R metric. With this dynamic way choice component, the CH guarantees that it can choose the most ideal way for information scattering. Figures demonstrate the outcomes when half of hubs are malignant. The throughput does not diminish in both conventions. At the point when vindictive hubs are on the steering way and don't forward bundles for the source, the proposed plan can distinguish this conduct as clarified in Section 4.3 in which different sorts of assaults can be guarded utilizing existing methods. Hub Resilience: In the nearness of half of the bargained hubs (very nearly 100 hubs out of 200 hubs taken) which drop all the re-laying parcels and promote conflicting directing data, the impact of proposed plan on a proportion of blocked hubs is appeared in Figure 6. Without the proposed plan, the impact of traded off hubs over the system is more since bargained hubs even pull in the system Traffic and drop them. Utilizing proposed plan, in any case,

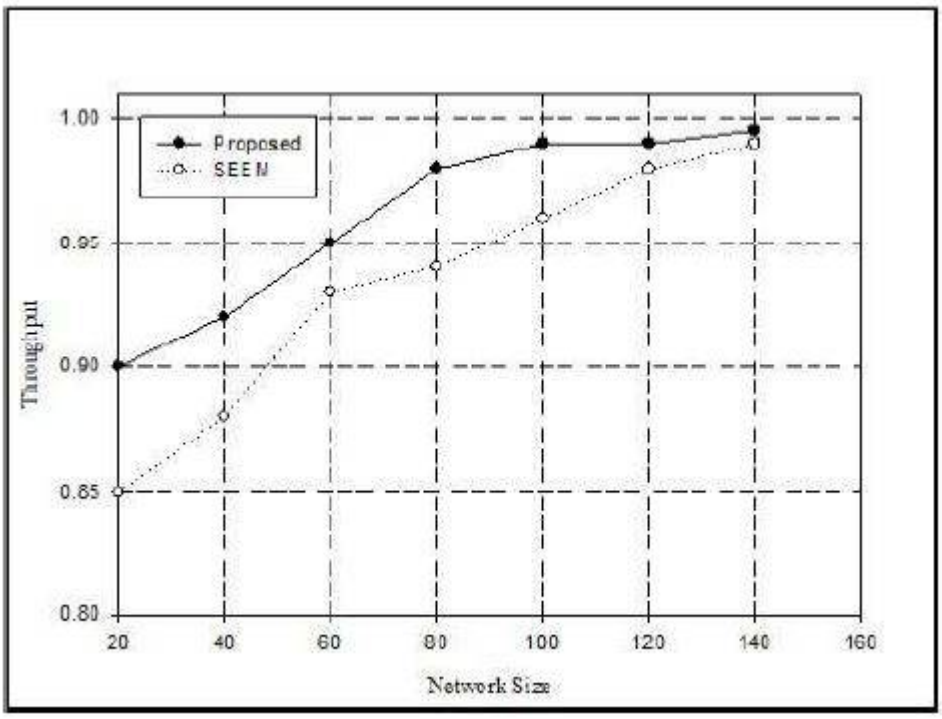


Figure 3: Throughput in SEEM and proposed scheme

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

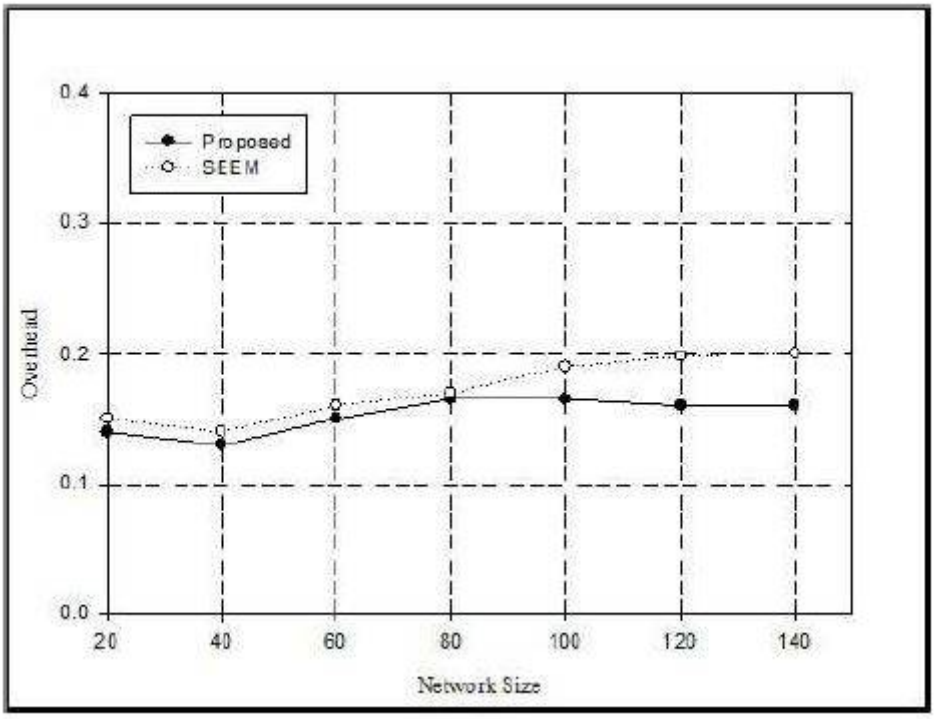


Figure 4: Control overhead in SEEM and proposed scheme Fi

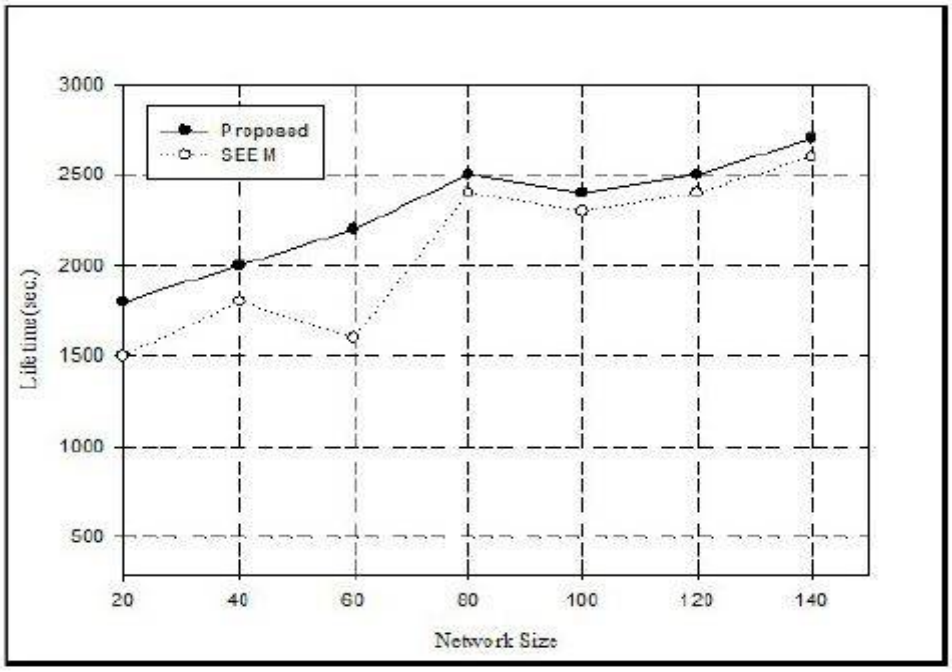


Figure 5: Network lifetime in SEEM and proposed scheme

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

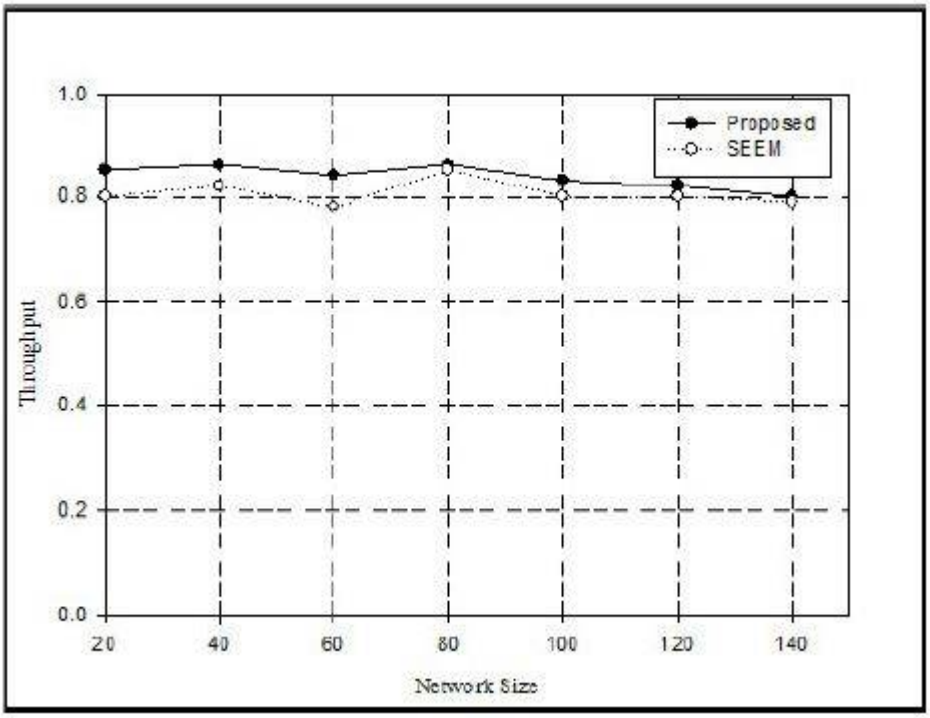


Figure 6: Throughput in SEEM and proposed scheme when the nodes are malicious

We can see that more than 90% of sensor nodes are not blocked. Legitimate nodes did not forward packets to the com promised nodes identified. Thus, with several compromised nodes, almost all of them are excluded from the network so that more than 90% of sensor nodes are not
Blocked. Also the routing path is selected by the respective CH, which periodically re-selects a new path according to R metric defend in Equation 1 along multipath. There- fore, whatever the compromised node advertises, it has no impact on routing path and cannot attract traffic through itself. Even if the compromised nodes are happened to be in the routing path, the attack lasts only for limited period. Hence the proposed scheme is quite effective against the wormhole and sinkhole attack.

## VII. CONCLUSION

This paper proposes a novel information revelation and scattering convention for remote sensor systems which can be utilized to accomplish secure and quick information dispersal particularly for little setup parameters and variables. This procedure consolidates the ideas of system coding and straightforward cryptographic methods in order to disperse information. The benefits of this convention are that it is impervious to contamination assaults, and accomplishes prompt confirmation of information been dispersed. Session keys are utilized to encode and send information in the middle of hubs and there is no need of real exchange of the session keys through the system. Likewise just basic scientific operations are utilized to compute keys for encryption of information so very little of asset use at the hubs. All together it plans to give a basic yet secure and quick information spread convention for utilization in remote sensor systems. Hub bargain by an assailant can be an issue in this convention. It will be managed as a major aspect without bounds works.

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

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 3, March 2016**

## REFERENCES

[1] Mohammad A. Matin, Wireless Sensor Networks: Technology and Protocols: Published by InTech, Croatia, ISBN 978-953-51-0735-4, 2012.
[2] Salvatore La Malfa, Wireless Sensor Networks, 2010.
[3] Jisha Mary Jose, Jomina John, "Data dissemination protocols in wireless sensor networks-a survey", IJARCCE, March 2014.
[4] T. Ho and D. Lun. Network Coding: An Introduction. Cambridge University Press, 2008.
[5] Daojing He, Sammy Chan, Shaohua Tang and Mohsen Guizani, "Secure Data Discovery and Dissemination based on Hash Tree for Wireless Sensor Networks", IEEE transactions on wireless communications, Vol. 12, No. 9, September 2013.
[6] P. Levis, N. Patel, D. Culler and S. Shenker, "Trickle: a self regulating algorithm for code maintenance and propagation in wireless sensor networks", in Proc. 2004 NSDI, pp. 15-28.
[7] G. Tolle and D. Culler, "Design of an application-cooperative management system for wireless sensor networks," in Proc. EWSN, pp. 121–132, 2005.
[8] Lin, K., Levis, P.: "Data discovery and dissemination with dip." In: Proceedings of the 2008 International Conference on Information Processing in Sensor Networks (IPSN 2008), Washington, DC, USA, IEEE Computer Society (2008) 433-444.
[9] T. Dang, N. Bulusu, W. Feng, and S. Park, "DHV: a code consistency maintenance protocol for multi-hop wireless sensor networks", in Proc. 2009 EWSN, pp. 327-342.
[10] Hui, J.W., Culler, D.: "The dynamic behaviour of a data dissemination protocol for network programming at scale." In: Proceedings of the 2nd international conference on Embedded networked sensor systems (Sensys 04), New York, NY, USA, ACM (2004) 81-94.
[11] Nildo dos Santos Ribeiro Junior, Marcos A. M. Vieira1, Luiz F. M. Vieira1 and 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.
[12] Hailun Tan, "Secure multi-hop network programming with multiple one-way key chains", In: Proceedings of the International conference on Embedded networked sensor systems (Sensys 07), Sydney, Australia, ACM.
[13] YingpeiZeng, Jiannong Cao, Shigeng Zhang, ShanqingGuo, Li Xie, "Pollution Attack: A New Attack Against Localization in Wireless Sensor Networks", IEEE, WCNC-2009.
[14] I-Hong Hou, Yu-En Tsai, T.F. Abdelzaher, and I. Gupta. Adapcode: Adaptive network coding for code updates in wireless sensor networks. In INFOCOM 2008.The 27th Conference on Computer Communications.IEEE, pages 1517–1525, 2008.
[15] Andrew Hagedorn, David Starobinski, and Ari Trachtenberg.Rateless deluge: Over-the-air programming of wireless sensor networks using random linear codes. In Proceedings of the 7th international conference on Information processing in sensor networks, IPSN '08, pages 457–466, Washington, DC, USA, 2008. IEEE Computer Society.
[16] S. Katti, H. Rahul,W. Hu, D. Katabi, M.Medard, and J. Crowcroft, "XORs in the air: practical wireless network coding", ACM SIGCOMM Computer Communication Review, vol. 36, no. 4, pp. 243-25, 2006.
[17] Philip Levis, Nelson Lee, Matt Welsh, and David Culler. "Tossim: accurate and scalable simulation of entire tinyos applications, In SenSys '03, pages 126-137, New York, NY, USA, 2003. ACM Press.
[18] TinyOS: an open-source OS for the networked sensor regime. Available: http://www.tinyos.net/.
[19] Simulating a Wireless Sensor Network, 2010-2013, [Online] Available: http://virtual-labs. ac.in/ cse28/ ant/ ant/8/theory/.