A Systematic Approach for the Secure and Dynamic Data Aggregation and Transmission in Wireless Sensor Networks

K.Niranjan[1] B.Rama Ganesh [2]

1. M.Tech Scholar, Department of Computer Science and Engineering, Vemu Institute of Technology, P.Kothakota, Chittoor,
2. Associate Professor, Department of Computer Science and Engineering, Vemu Institute of Technology, P.Kothakota, Chittoor ,

Abstract:-*Remote sensor systems (WSN) are fundamentally dispersed systems or a gathering of sensor hubs which gather data which are utilized to break down physical or natural conditions. WSNs are generally setup in remote and antagonistic territories and work in great conditions. Uses of WSN incorporate natural surroundings checking, modern applications, combat zone reconnaissance, savvy homes and so on. The greater part of them require standard redesigning of programming in sensor hubs through the remote channel for productive administration and working. So it is important to spread information through the remote medium after the hubs are sent. This is known as information scattering or system reconstructing. A decent information scattering convention must be quick, secure, dependable and vitality effective. To accomplish these we can make utilization of system coding procedures which decreases the quantity of retransmissions because of any parcel drops. Be that as it may, network coding expands the possibility of different sorts of system assaults. Likewise to abstain from spreading of malevolent code in the system, every sensor hub needs to verify its got code before engendering it further. So here a novel spread convention is presented taking into account straightforward cryptographic procedures which anticipates contamination and DoS assaults and in the meantime accomplishes quickness utilizing the strategy of system coding*

I.INTRODUCTION

Remote Sensor Networks (WSN) is one of the major turning points in the field of correspondence . These organized accumulation of hubs make us a stride nearer to getting profitable data about the physical world. WSN are utilized prevalently as a part of numerous applications like remote control and observing, development security frameworks, ecologicalobserving, medicinal services administration, debacle administration, reconnaissance operations, keen homes, territory checking, indoor sensor systems, seismic observing of structures and so forth [1]. In software engineering and correspondence remote sensor systems stimulate part of examination today.

A WSN is made of sensor hubs utilized for observing and investigation purposes as appeared in Fig 1.

These sensor hubs pass the data that they gather to a prime area called a base station. In many frameworks, a WSN speaks with a LAN or WAN through an entryway like medium. The entryway is really an extension between the WSN what's more, the different systems [2]. This permits information to be put away by gadgets and which can be taken up for preparing later. Every sensor hub or bit has a few sections: a circuit for interfacing with other sensor hubs, a miniaturized scale controller, a radio handset, and a battery for force supply. The topology utilized can be either a star, ring, lattice system or multi-bounce remote cross section network.WSN is utilized principally as a part of remote and antagonistic situations for data gathering.

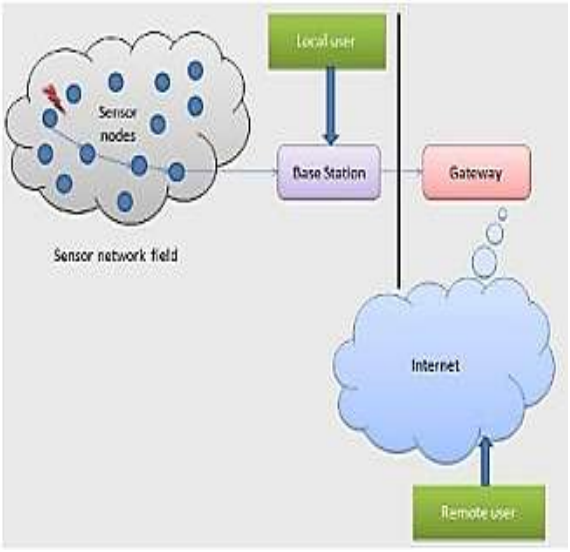

Fig 1: Dissemination on the Network

Consequently it is a noteworthy test to create shoddy sensor hubs. They should be composed deliberately by considering all the diverse limitations of the earth in thought. Remote sensor systems must be worked for long term of time and for the most part don't get any human organization or mediation in the middle of [3]. Developing conditions and situations can likewise; cause changes in application highlights, which subsequently prompt the need to change the system conduct by presenting new code or programming. Be that as it may, the remote nature of WSN is a burden here. It will require the engendering of new code upgrades over the remote medium i.e. over the air as manual overhauling of such systems won't be conceivable.

This procedure is known as spread or system reinventing. Be that as it may, scattering acquires a ton of difficulties [3]. One significant test is legitimate and finish spread of data to all sensor hubs in the system. This istroublesome since the quantity of hubs in the system can be immense and the earth is constantly changing, consequently the fundamental topology continues evolving always. Secondly 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 secury or else foes can track out basic information. Likewise there is a plausibility of aggressors sending false information into the system which must not be gotten by the sensor hubs as they can bring about various assaults like contamination assaults, refusal of administration assaults etc.

So spread of code or program information in remote sensor systems is a zone to be worked in profoundly and new strategies should be acquainted with accomplish tradeoffs amongst vitality and velocity in spread. The point of this work is to build up a novel secure and quick information spread convention for use in remote sensor systems. This work focuses on building up a scattering convention for scattering of little information.

Direct system coding is a strategy used to accomplish quickness and vitality productivity amid spread [4]. It is a system that joins bundles in the system; expanding the throughput, diminishing vitality utilization, a lessening the quantity of messages transmitted. In customary frameworks dropped parcels are recouped utilizing retransmissions. Yet, in system coding we can join parcels utilizing scientific operations and afterward spread so that recuperation of lost parcels can be accomplished without retransmission.

Yet, arrange coding alongside its vitality effectiveness points of interest acquires a considerable measure of cerebral pains. It is very inclined to assaults like contamination, refusal of-administration assaults and numerous others. So to manage these the proposed framework employments basic yet productive cryptographic procedures for information scattering. This ensures we can accomplish straightforward however secure information scattering in remote sensor systems.

Our work is sorted out as takes after. To begin with we concentrate on the need of information dispersal in remote sensor systems and a few

of its related works. Next the configuration and usage which focuses on the spread of little values and variables is clarified. At that point we concentrate on the execution of the new convention through broad recreation utilizing TinyOS lastly have the conclusion and references.

II. RELATED STUDY

Information scattering in remote sensor systems is a basic what's more, crucial assignment. It depends on the idea of customary correspondence framework, where we have a sender and beneficiary. The situation is essentially a sender conveying some data, and beneficiary gathering the data sent, preparing it and sending some data back. While in information dispersal, just 50% of this idea is connected. Some data is conveyed and got at the destination, yet no answer is given back. The sender conveys data, not to one hub, but rather to numerous as in a television framework.

Spread 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 redesigning of sensor hubs conveyed in remote situations is beside incomprehensible in the greater part of the cases. The principle point of a spread convention in WSN is to guarantee that all the sensor hubs have steady information with them continuously.

There are two sorts of dispersal in WSN [5]:

A] Code dispersal - to send program pictures which are for the most part massive information. Typically they are isolated into altered estimated pages and parcels and after that dispersed.

B] Data revelation and spread - to scatter little design parameters, variables, inquiries, charges and so on in parcels.

2.1 Small Value Dissemination

This work focuses on information disclosure and dispersal conventions i.e. scattering of little values like variables, parameters et cetera. Figure 2 gives a general thought regarding information spread. Conventional conventions accessible for this incorporate Drip, DIP and DHV. They are all in light of Trickle calculation [6].

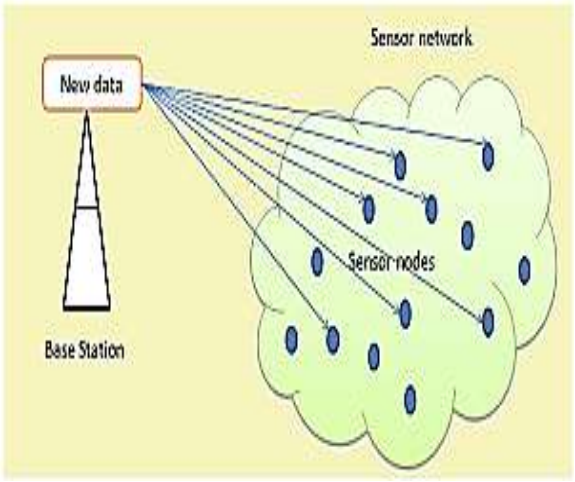

Fig 2: Wireless Sensor Networks Dissemination

Dribble proposed by Tolle et. al [7] is the most straightforward of all spread conventions and depends on Trickle calculation also, builds up a free stream for every variable in the information. Each time an application needs to transmit a message, another form number is produced and utilized. This will bring about the convention to reset the Trickle clock and in this mannerscatter the new esteem else the stream clock interim is augmented.

Plunge (Dissemination Protocol) [8] is an information location and scattering convention proposed by Lin et al. It is a convention taking into account 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 is taking into account the idea of adaptation number and key tuple for every information thing. Plunge ascertains hashes that cover all form quantities of the information. Hubs th at get hashes same as their own realize that they have steady information regarding their closest neighbors. On the off chance that a hub gets a hash that varies from its own hash, it realizes that a distinction exists in the information.

DHV (Difference recognition Horizontal pursuit Vertical look), [9] is a code consistency support convention given by Dang et al. It tries to keep codes on various hubs in a WSN predictable and exceptional. Here likewise information things are spoken to as tuples (key, rendition). It depends on the

perception that if two information things are distinctive, they will just contrast in a couple of slightest noteworthy bits (LSB) of their rendition number as opposed to in every one of their bits. So just those bits should be checked. For this strides took after are discovery what's more, recognizable proof.

There are numerous code dispersal conventions like Deluge [10] too. They are utilized to scatter expansive code upgrades into the system. For this the code is frequently broken down into pages and after that further into bundles. Here we have seen some fundamental information revelation and dispersal conventions. They don't bolster any procedures which help to diminish parcel retransmissions. Likewise none of these conventions give security to the information dispersed.

2.2 Network Coding and Data Dissemination

System coding [4] means to supplant the customary store and forward method utilized as a part of systems; by better steering calculations that will permit halfway hubs to changethe moving information. System coding has gotten to be prominent due to its properties like strength and better throughput. It accomplishes quick information spread as it lessens the number of retransmissions that will be required if there are parcel misfortunes.

Numerous spread conventions have been created utilizing the idea of system coding [14] [15]. The upsides of system coding based spread conventions are that they accomplish vitality investment funds and correspondence productivity, particularly amid expanded parcel misfortune or system thickness. So organize coding based conventions can be gainful for reinventing of WSNs. Nonetheless we confront a potential issue in threatening situations. A foe may dispatch contamination assaults, in which a vindictive hub sends awful encoded bundles that comprise of counterfeit information, which prompts mistaken unraveling of the first information upon recovery.

Here we utilize paired system coding i.e. the scientific operation utilized is XOR to join the substance of parcels [4]. Just two parcel system coding is done here.

Likewise here concentrated on scattering of little values like setup parameters, variables, inquiries, orders and so on whose size range from 2-4 bytes and accordingly is alteration of the current Dribble convention.

3. Presumptions and Threat Model

3.1 Assumptions

Here accept that the wellspring of the reconstructing variables, i.e., the base station, is a protected area. Additionally every sensor hub has a special ID number. We accept that while every sensor hub is asset restricted, it has adequate memory to store all the security components of the convention.

3.2 Threat Model

Here accept that the individual sensor - hubs are unprotected. An enemy may embed its own particular aggressor hubs into the system, or it might catch different hubs. The enemy can endeavor to dispatch contamination assaults to degenerate the information in the system furthermore to devour the restricted assets on sensor hubs.

III. PROPOSED SYSTEM

In this convention information spread is done in a protected and quick path by utilizing the methods of system coding and cryptography. System coding lessens the quantity of retransmissions because of any bundle misfortunes happening in the system by brushing and sending information. Likewise information scattered is constantly sent as encoded information.

For this hubs first perform hub to hub validation and set up session keys. At that point the session key is utilized for encoded exchange of information. This convention guarantees that the framework is free of contamination [13] and Denial-of-Service assaults. The diverse periods of this convention include:

4.1 System Initialization Phase

This stage is done before the WSN is conveyed in the application field. In this stage the base station produces a expert key Km what's more, an exceptional irregular number Rm what's more, stores

them securely in every hub. Likewise a rundown of all the substantial hub ids is kept up in every hub.

4.2 Packet Processing Phase

In this stage the genuine information dispersal happens. Sometime recently dispersing information a hub will produce a constant key utilizing a key era calculation. This incorporates the era of two extraordinary arbitrary numbers R1_node and R2_node. Key era is done utilizing Trivium-Multilinear Measured Hashing (MMH) as the MAC capacity and SHA1 as hashing capacity H(x). The strides 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 expert key of the MAC capacity, node_id is the identifier of the comparing hub, XOR is the coherent XOR operation. This constant key is show by the hub in a bundle which will incorporate the node_id and the key. The destination hub who gets it will check the node_id with its rundown of legitimate hubs and guarantee this parcel is originating from a substantial hub.

On the off chance that yes that hub will likewise create a constant key utilizing the same procedure as above and send back an answer parcel to the sender hub which will contain the node_id and the recently produced key.

On the off chance that this parcel is likewise accepted, then the two hubs are prepared to create a session key.

The key is produced as:

Session key = K

m XOR Ka XOR Kb (5)

Where Ka and K b are keys created at any two hubs An and B. Presently this key is utilized for scrambling the information to be spread. The benefit of this plan is that there is no need of real trade of the session key through the system. To scramble the information we utilize symmetric encryption methods ideally Advanced Encryption Standard (AES). So the information bundle dispersed from a hub will contain the information in scrambled structure i.e.

Information = E (d)sk

, where sk is the session key. (6)Dispersal in remote sensor systems chips away at the premise of Trickle calculation [2]. It tackles the idea oftattling. At whatever point another information is to be spread the stream clock is reset to 0 and the information is telecasted. Whenever a hub gets another information it will store it. Be that as it may, in the event that it gets a information which it as of now knows about then it will expand the stream clock interim and stifles the copy approaching information.

To accomplish prompt confirmation of information bundles a onetime hash of the at first created arbitrary number is additionally computed and incorporated into every parcel. The strides are:

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

2. Result = ADD(Hash) (8)

Where H( ) is SHA-1 and ADD( ) is essential option operation. The outcome is incorporated into the parcels sent.

4.3 Packet Verification Phase

To accomplish prompt validation of the got parcel,

the destination hub will figure the hash of R mput away in its memory and contrast it and the worth in the got parcel. In the event that they coordinate, then they got bundle is a substantial hub. Hence it will be recognized ACK by the destination.

Generally a NACK (negative ack) is sent to the sender. Next we will need to guarantee the trustworthiness of the information. For this to begin with the hub checks the id in the got parcel. On the off chance that it is a substantial node_id, then it will endeavor to decode the information utilizing the session key as of now produced and put away. Each hub has a unique information and joined information cradle. So the hub will check whether it is a unique

information or joined information. On the off chance that it is a unique information it will be put away and spread after a stream clock fire and in the event that it is a joined information, the hub will check whether it is conceivable to extricate whatever other information from this recently got information utilizing system coding.

After that the information will be put away or spread out. So in like manner every one of the information dispersed from the first source hub will be circulated to every one of the hubs and a round of scattering will be finished. This system in this manner ensures that lone substantial information is conveyed and information is beenconveyed securely.

IV.EXPERIMENTAL RESULTS

This convention has been executed in TinyOS-2.1.2 test system TOSSIM [17]. We have considered a system topology comprising of 100 hubs and 25 unique information variables are scattered. The parcel size in TinyOS [18] is 29bytes. The sensor hub considered for reproduction here is micaz. Cryptographic backing has been accomplished utilizing hashing

calculations like SHA-1 which produces a 160 piece hash esteem, Macintosh capacities like TriviumMultilinear Modular Hashing (MMH), and symmetric encryption calculations like AES which utilizes a 128 piece key.

The new convention is found to oppose instances of contamination assaults i.e. just legitimate information bundles are gotten and handled by the middle of the road hubs in the system. Additionally prompt confirmation of bundles is accomplished utilizing the one time hash esteem produced and put away in the information parcels dispersed.

V. SECURITY AND PERFORMANCE ANALYSIS

To start with we perform and examine the security offered by this convention. Resistance to contamination assaults Attackers can't dirty the system with false information since information exchange done is constantly checked utilizing cryptographic procedures.

A] Resistance to Denial-of-Service assaults Immediate confirmation of parcels is done at every destination, so false parcels can be disposed of and just substantial parcels go through.

B] Session key understanding Session keys are utilized for encryption and decoding. Likewise this key is locally produced and utilized, thus not traded in the system.

C] Real time key era No-pre put away keys in hubs; they are figured at time of information exchange as it were.

D] Light-weight-Only straightforward yet great scientific operations and encryptions methods are utilized henceforth no much asset utilization in hubs. Outline 1 gives an examination diagram on the quantity of information messages spread in every convention specifically DRIP [7], CodeDrip [11] and the new proposed convention. Systemcoding has lessened aggregate number of messages.

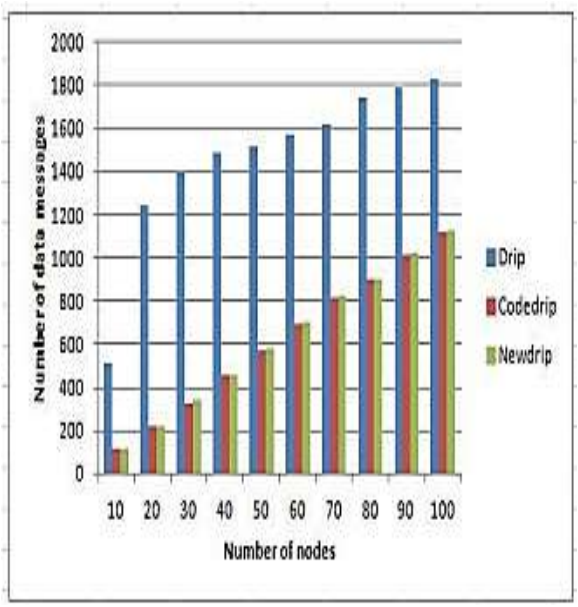

Chart 1: Statistics of the Messages Disseminated

VI. CONCLUSION

This paper proposes a novel information disclosure and scattering convention for remote sensor systems which can be utilized to accomplish secure and quick information scattering particularly for little setup parameters and variables. This system joins the ideas

of system coding furthermore, basic cryptographic systems in order to disperse information. The upsides of this convention are that it is impervious to contamination assaults, and accomplishes quick confirmation of information been dispersed. Session keys are utilized to encode what's more, send information amongst hubs and there is no need of genuine exchange of the session keys through the system. Additionally as it were straightforward scientific operations are utilized to ascertain keys for encryption of information so very little of asset utilization at the hubs. All together it intends to give a straightforward yet secure also, quick information spread convention for utilization in remote sensor systems. Hub trade off by an aggressor can be an issue in this convention. It will be managed as a feature of the future works.

VII. 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 Processingin 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 onWireless 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 ComputerCommunications.IEEE, pages 1517–1525, 2008.

[15] AndrewHagedorn, 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,

[16]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.

AUTHOR PROFILE

K.Niranjan is currently a M.Tech Scholar in Department of Computer Science and Engineering, Vemu Institute of Technology, Chittoor, He completed his B.Tech in Information Technology from Kuppam Engineering College, JNTU Anantapur in 2011. His current area of Interest is Networking and Administration.

B.Ramaganesh Received his M.Tech degree in Computer Science & Engineering and B.tech in Computer Science and Information Technology, both from JNTUH University, P.hd degree Pursuing in Vignan University , Guntur. Where he is now an Assoc.prof of & HOD in the Department of Computer Science & Engineering in VEMU Institute of Technology, Chittoor (dt), Presently he serves as Dean of Academics of VEMU Institute of Technology, during from 2012 onwards. His Research interests are in the areas of Software Engineering, Computer Organization, DWDM, Software Project Management, and A.I. And he has 11 Years Teaching Experience in this field.