INTERNATIONAL JOURNAL OF RESEARCH
In Advanced Engineering Technologies

Volume 5, Issue 3 MAY 2016

DATA DETECTION AND DISTRIBUTION IN WSNS BY USING DIDRIP TECHNIQUE

[1] Dr.G. VENKATA RAMI REDDY, [2] B. SYAMALA

[1] Associate Professor, School of Information Technology JNTUH, Kukatpally, Hyderabad, Telangana State, India.

2 Assistant Professor, Department Of CSE, Vasavi College of Engineering, Ibrahimbagh, Hyderabad, Telangana State,India.

Abstract*— *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. 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:DTNs, CP-ABE, data retrieval,requirements, cipher text, attributes.

I. INTRODUCTION

A wireless detector network (WSN) is created of a group of nodes and is employed for watching and analysis purposes. the data collected through the network is given to a main location called a base station. the appearance of wireless detector networks was motivated chiefly by military and industrial applications. however nowadays detector networks are used popularly in several applications like environmental monitoring, attention systems, disaster management etc. The WSN consists of nodes variable from some to several thousands, wherever every node is connected to several alternative nodes. every node has many elements like a microcontroller, a radio transceiver, interface with sensors and electric battery for power offer. Sensor networks ar sometimes setup in remote and hostile environments. thus there ar several constraints on resources like value, size, procedure speed, energy, memory & information measure. The topology of WSNs can be a star network or a mesh network counting on the corresponding application space.

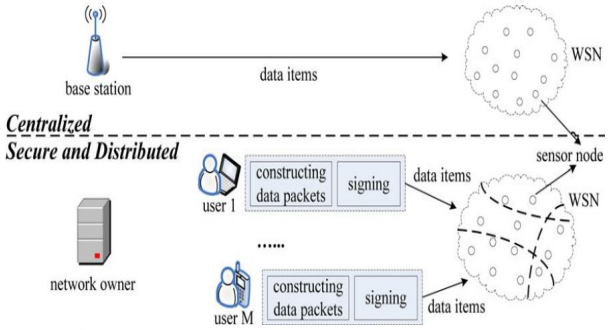


Fig. 1. System overview of centralized and distributed data discovery and dissemination approaches.

Wireless device networks should sometimes operate for long periods of your time and do not get any human administration or intervention. conjointly evolving conditions and atmosphere will amendment application requirements, inflicting the necessity to change the behavior of the network by introducing new code or updates. The remote nature of WSNs needs the propagation of new code over the network i.e. through air; as manual change of such networks is not possible. This process of reprogramming a WSN is understood as dissemination. Dissemination protocols in WSN area unit based on Trickle algorithmic rule.

There square measure several common dissemination protocols available for wireless sensing element networks. they'll be broadly classified into code dissemination and knowledge discovery and dissemination. 1st one is employed to disseminate giant code updates as a full therefore on reprogram the software package in a very sensing element node. Data discovery and dissemination protocols square measure accustomed disseminate tiny commands, parameters, queries, variables etc. Existing protocols like Drip, Dip and DHV square measure ancient and have a problem of been not secured. Any somebody are able to create use of those protocols to circularize bogus knowledge into the network. to forestall this several secure dissemination protocols were introduced. Here we've got a comparison of a number of the secure dissemination protocols used these days in wireless sensor networks. the remainder of the paper is organized as follows. In section II a number of the presently enforced secure dissemination protocols square measure mentioned. Section III gives a comparison of the protocols. The paper ends with a conclusion and references.

II. Related Work

2.1. Seluge

This paper planned by Hyun et. al, presents an economical, secure, robust, and DoS-resistant code dissemination protocol named Seluge for wireless sensor networks. it's a secure extension to Deluge protocol, associate degree open ASCII text file dissemination system for WSN. It provides security protection for code update dissemination, which has integrity protection for code pictures and protection from all kinds of DoS attacks that attack code dissemination protocols. The key contribution of Seluge may be a thanks to organize the packets wont to distribute new code images. By fastidiously handling code dissemination data things and their hash pictures in packets, this protocol provides immediate authentication of every data packet upon reception, while not disrupting the efficient propagation mechanisms that ar utilized by Deluge. It will so defeat the Denial of Service attacks that exploit authentication delays. Seluge uses a signature to bootstrap the authentication of a new code image. However, not like different protocols, it uses a weak authentication beside the signature.

2.2. Se-Drip

This paper planned by Huayang et. al could be a secure extension to the Drip dissemination protocol. Se-Drip (Secure Drip) could be a secure, light weight, DoS resistant knowledge discovery and dissemination protocol. it's used for dissemination of tiny configuration parameters, variables, commands etc. It ensures security by mistreatment the concepts of Elliptic curve cryptography and Merkle hash tree. This protocol consists of 3 phases. System initialization, packet pre-processing and packet verification section. within the 1st section elliptic curve cryptography is setup and also the keys ar pre-deployed in the device nodes. within the next section knowledge to be disseminated ar wont to construct a merkle hash tree whose root is signed mistreatment ECC. This acts as a signature packet. knowledge received at every node is verified by mistreatment the contents of the signature packet and solely then is accepted. therefore attackers can't send bogus knowledge to nodes. This protocol therefore helps to maintain integrity of information things, forestall DoS attacks etc.

2.3. Sluice

Sluice is associate extension to the normal dissemination protocols and facilitates the secure dissemination of program updates. This protocol was proposed by Apostle et. Sluice ensures that only trusty and verified updates square measure disseminated in wireless sensing element networks, whereas malicious updates are stopped from propagation within the network as shown below. This ensures that the compromise of any sensing element node won't result in the execution of malicious code on the other uncompromised node.

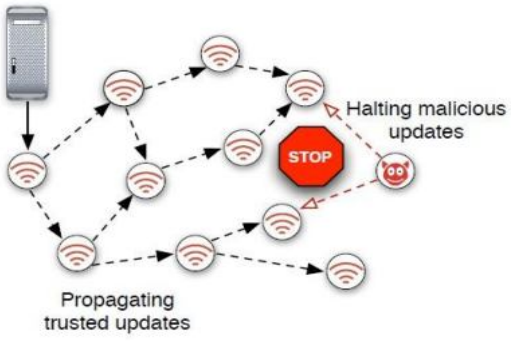


Figure 2: Sluice operation

This protocol respects the resource affected nature of

detector nodes and supports the utilization of existing potency mechanisms. therefore its verification is each resource-sensitive and progressive in nature. Sluice divides a code update into mounted sized pages for dissemination. thus it uses progressive verification technique here. to realize this, combination of digital signatures and off-line hash chains is followed. the essential plan is to form a sequence of hashes, by computing a hash of every page and incorporating that hash as a vicinity of the previous page's payload. Then digitally sign the primary page in the chain; therefore, there'll be hash price for every page, however just one digital signature for each set of pages that type Associate in Nursing update for dissemination. So the digital signature are verified in every dissemination to visualize the validity of information.

2.4. SAFE

This protocol projected by Kim et. al is utilised for dissemination in layer networks that consist of stationary detector nodes and mobile knowledge users WHO request periodic detector knowledge updates. SAFE (Sinks Accessing knowledge From Environments) is a data dissemination protocol for wireless detector networks. victimization SAFE protocol, individual detector observations are often disseminated into knowledge sinks or the base station WHO expressly gift their interests by causing out knowledge requests. every knowledge sink is allowed to specify its own desired knowledge update rate, and then SAFE can confirm a subscription purpose through that the sink will get updated, trying to reduce the amount of message transfers within the entire network.

2.5. Secure Code Distribution in Dynamically Programmable Wireless Sensor Networks

This technique planned by Deng et. Gives prime importance to safe and secure reprogramming of wireless detector networks. To avoid reprogramming with false or phoney code pictures in the network, it's important to form certain that every sensor node receives its code image properly through the wireless network. Here public key operations victimization Elliptic Curve Cryptography and hashing schemes square measure used to produce secure data dissemination. during this paper 3 schemes for secure and safe code propagation square measure given. 1st is that the chain based mostly scheme that works best once packets square measure received in the order they were sent with only a few losses. Next is that the hash tree based mostly theme that permits nodes to attest packets and verify their integrity quickly, even though the packets arrive out of order. Finally is that the hybrid theme which mixes the advantages of the primary two schemes, and any reduces memory usage and range of public key operations that a node has got to perform.

2.6. DiCode

Almost all the code dissemination protocols seen till currently area unit centralized in nature i.e. they take into account a single base station that disseminates knowledge or code into the detector network. during this paper projected by Daojing He et al. dissemination of code pictures occurs in an exceedingly distributed manner that permits multiple network users to at the same time update code pictures on totally different nodes while not involving the bottom station. Also this dissemination protocol is denial of service attack resistant. A distributed code dissemination protocol consists of 3 sorts of participants, the network owner, verified network users and detector nodes. After the network users register to the network owner, they'll enter to into the WSN and so have privileges to directly reprogram the detector nodes without involving the owner itself. to realize this cryptographic technique may be used. during this paper PSW (proxy signature by warrant) technique is employed. The network owner plays the role of original signer while the network users play the role of proxy signers. By registering, the users get one or a lot of proxy signature keys from the network owner before they enter the WSN. The keys will then be accustomed make a signature on a new code image sent to the sensor nodes.

III. FRAME WORK

In this protocol information dissemination is finished in a very secure and fast manner by victimization the techniques of network cryptography and cryptography. Network cryptography reduces the quantity of retransmissions attributable to any packet losses happening within the network by hairdressing and causing information. Also data disseminated is often sent as encrypted information. For this

nodes 1st perform node to node authentication and establish session keys. Then the session key's used for encrypted transfer of knowledge. This protocol ensures that the system is freed from pollution and Denial-of-Service attacks. the various phases of this protocol include:

3.1 System Initialization Phase

This section is finished before the WSN is deployed within the application field. during this section the bottom station generates a master key klick and a novel random range Rm and stores them safely in every node. conjointly an inventory of all the valid node ids is maintained in every node.

3.2 Packet Processing Phase

In this section the particular information dissemination happens. Before disseminating information a node can generate a true time key using a key generation algorithmic rule. This includes the generation of 2 distinctive random numbers R1_node and R2_node. Key generation is finished victimization Trivium-Multilinear Modular Hashing (MMH) because the waterproof perform and SHA1 as hashing perform H(x). The steps are:

1. $MAC[i] = R_1\_node \text{ XOR } K[i]$ (1)
2. $a[i] = node\_id + MAC[i]$ (2)
3. $h = MMH (a[i])$ (3)
4. $Key = H (h \text{ XOR } R_2\_node)$ (4)

Where K[i] is that the passe-partout of the mack perform, node_id is the symbol of the corresponding node, XOR is the logical XOR operation. This real time secret's broadcast by the node in a very packet which is able to embody the node_id and also the key. The destination node WHO receives it'll check the node_id with its list of valid nodes and guarantee this packet is coming from a sound node. If affirmative that node also will generate a real time key victimization identical method as on top of and send back a reply packet to the sender node which is able to contain the node_id and also the fresh generated key.

If this packet is additionally valid, then the two nodes area unit prepared to generate a session key. The secret is generated as:

$$\text{Session key} = K_m \text{ XOR } K_a \text{ XOR } K_b \quad (5)$$

Where Ka and computer memory unit area unit keys generated at any two nodes A and B. currently this secret is used for encrypting the information to be disseminated. The advantage of this theme is that there's no would like of actual exchange of the session key through the network. To write the information we tend to use radial secret writing techniques ideally Advanced secret writing customary (AES). therefore the knowledge packet disseminated from a node can contain the information in encrypted kind i.e.

$$Data = E (d)_{sk} \text{ , where sk is the session key.} \quad (6)$$

Dissemination in wireless detector networks works on thebasis of Trickle algorithmic rule. It takes on the construct of gossiping. Whenever a brand new information is to be disseminated the trickle timer is reset to zero and also the information is broadcasted. When a node receives a brand new information it'll store it. however if it receives a data that it already is responsive to then it'll increase the trickle timer interval and suppresses the duplicate incoming data. To achieve immediate authentication of information packets a onetime hash of the ab initio generated random range is also calculated and enclosed in every packet. The steps are:

1. $\text{Calculate Hash} = H(R_m)$ (7)
2. $\text{Result} = ADD(\text{Hash})$ (8)

Where H( ) is SHA-1 and ADD( ) is basic addition operation. The result is included in the packets sent.

3.3 Packet Verification Phase

Toknow the current authentication-details of the received packet, the destination node can calculate the hash of Rm keep in its memory and compare it with the worth within the received packet. If they match, then the received packet could be a valid node. therefore it'll be acknowledged ACK by the destination. Otherwise a NACK (negative ack) is distributed to the sender. Next we'll need to make sure the integrity of the information. For this first the node checks the id within the received packet. If it is a valid node_id, then it'll plan to rewrite the information mistreatment the session key already generated and keep. Every node has a resourceful knowledge and combined knowledge buffer. therefore the node will check whether or not it's a resourceful knowledge or combined knowledge. If it is a resourceful knowledge it'll be keep and disseminated once a trickle timer hearth and if it's a combined knowledge, the node can check whether or not it's attainable to extract the other knowledge from this new received knowledge mistreatment network cryptography. After that the data are going to be keep or disseminated out.

So likewise all the information disseminated from the initial source node are going to be distributed to any or all the nodes and a spherical of dissemination are going to be completed. this method therefore makes positive that solely valid knowledge is distributed out and knowledge is been sent out safely.

3.4 Implementation Details

This protocol has been enforced in TinyOS-2.1.2 simulator TOSSIM . we've thought-about a network topology consisting of one hundred nodes and twenty five completely different information variables square measure disseminated. The packet size in TinyOS is 29bytes. The device node thought-about for simulation here is micaz. Cryptographic support has been achieved victimisation hashing algorithms like SHA-1 that generates a a hundred and sixty bit hash price,

MAC functions like Trivium Multilinear standard Hashing (MMH), and rhombohedral secret writing algorithms like AES which uses a 128 bit key. The new protocol is found to resist cases of pollution attacks i.e. solely valid information packets square measure received and processed by the intermediate nodes within the network. additionally immediate authentication of packets is achieved victimisation the only once hash price generated and keep within the information packets disseminated.

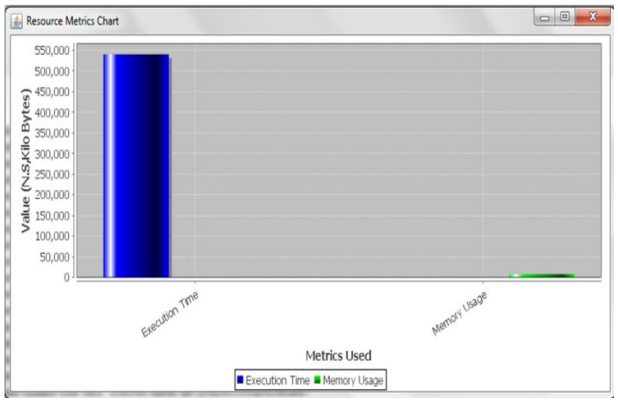
IV. Experimental Results

First we tend to perform and analyze the protection offered by this protocol.

- Resistance to pollution attacks- Attackers can't pollute the network with bastard knowledge since knowledge transfer done is usually verified victimization cryptologic techniques.
- Resistance to Denial-of-Service attacks- Immediate authentication of packets is completed at every destination, so bastard packets are often discarded and solely valid packets experience.
- Session key agreement- Session keys square measure used for encryption and decoding. conjointly this secret's regionally generated and used, thence not changed within the network.
- Real time key generation- No-pre keep keys in nodes; they're calculated at time of information transfer only.

```
Your issue command is 25-65
Cipher first part 62,160
Cipher second part 214,80
Generated value 49 from node 2 user command verified with SHA 7e3829ef78d9fe7d07254a26155ccac42381dce7
Generated value 44 from node 0 user command verified with SHA 7e3829ef78d9fe7d07254a26155ccac42381dce7
Generated value 51 from node 3 user command verified with SHA 7e3829ef78d9fe7d07254a26155ccac42381dce7
Generated value 44 from node 3 user command verified with SHA 7e3829ef78d9fe7d07254a26155ccac42381dce7
Generated value 52 from node 3 user command verified with SHA 7e3829ef78d9fe7d07254a26155ccac42381dce7
Generated value 30 from node 2 user command verified with SHA 7e3829ef78d9fe7d07254a26155ccac42381dce7
Generated value 53 from node 1 user command verified with SHA 7e3829ef78d9fe7d07254a26155ccac42381dce7
Generated value 62 from node 1 user command verified with SHA 7e3829ef78d9fe7d07254a26155ccac42381dce7
Generated value 58 from node 3 user command verified with SHA 7e3829ef78d9fe7d07254a26155ccac42381dce7
Generated value 64 from node 2 user command verified with SHA 7e3829ef78d9fe7d07254a26155ccac42381dce7
Generated value 40 from node 4 user command verified with SHA 7e3829ef78d9fe7d07254a26155ccac42381dce7
Generated value 50 from node 3 user command verified with SHA 7e3829ef78d9fe7d07254a26155ccac42381dce7
Generated value 26 from node 1 user command verified with SHA 7e3829ef78d9fe7d07254a26155ccac42381dce7
Generated value 49 from node 0 user command verified with SHA 7e3829ef78d9fe7d07254a26155ccac42381dce7
Generated value 38 from node 3 user command verified with SHA 7e3829ef78d9fe7d07254a26155ccac42381dce7
Generated value 54 from node 2 user command verified with SHA 7e3829ef78d9fe7d07254a26155ccac42381dce7
Generated value 29 from node 0 user command verified with SHA 7e3829ef78d9fe7d07254a26155ccac42381dce7
Generated value 32 from node 1 user command verified with SHA 7e3829ef78d9fe7d07254a26155ccac42381dce7
Generated value 38 from node 2 user command verified with SHA 7e3829ef78d9fe7d07254a26155ccac42381dce7
Generated value 57 from node 1 user command verified with SHA 7e3829ef78d9fe7d07254a26155ccac42381dce7
Generated value 28 from node 3 user command verified with SHA 7e3829ef78d9fe7d07254a26155ccac42381dce7
Generated value 62 from node 4 user command verified with SHA 7e3829ef78d9fe7d07254a26155ccac42381dce7
Generated value 30 from node 3 user command verified with SHA 7e3829ef78d9fe7d07254a26155ccac42381dce7
Generated value 62 from node 4 user command verified with SHA 7e3829ef78d9fe7d07254a26155ccac42381dce7
Generated value 45 from node 0 user command verified with SHA 7e3829ef78d9fe7d07254a26155ccac42381dce7
Generated value 46 from node 3 user command verified with SHA 7e3829ef78d9fe7d07254a26155ccac42381dce7
```

Chart one provides a comparison graph on the quantity of information messages disseminated in every protocol specifically DRIP, CodeDrip and also the new projected protocol. Network coding has reduced total range of messages.



V. Conclusion

Here we proposed an advanced data discovery & dissemination method over WSNs which is providing a fast and confidential data dissemination. Mainly it is used for small configuration variables and parameters. Here the technique used to disseminate the data by combining network coding and simple cryptographic methods. The main usages of this technique are mainly protects from pollusion attacks and finds current authentication of data dissemination. Here it uses session keys to encrypt the data and to transmit the data between nodes also they are using same session keys. Here we need to know that no need for real transformation of session keys. Also used normal mathematical operations were used to calculate the encryption keys for data for decrease the usage of resources at the nodes. Simply we can say that the its main aim to provide a secure, simple and fast data dissemination technique for the usage of WSNs.

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 applicationcooperative 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 multihop 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] Yingpei Zeng, Jiannong Cao, Shigeng Zhang, Shanqing Guo, 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