International Journal of Science Engineering and Advance Technology

Enhanced Secure Dissemination with DIP and Data Discovery protocol in Wireless Sensor Networks

B.Manikumar [1], Kesavarao Seerapu [2]

#1. M.Tech (CSE) in Department of Computer Science Engineering,

#2. Assist.Prof, Department of Computer Science and Engineering, Institute Of Information Technology & Sciences, Visakhapatnam AP, INDIA.

Abstract

In Wireless sensor Network, the security of data is an important aspect.We present DIPanddatadiscovery and spread convention for wireless networks. Earlier methodologies, for example, Trickle or SPIN, have overheads that scale straightly with the quantity of data things. For T things, DIP can recognize new things with 0(log(T)) parcels while keeping up an O(l) identification inertness. To accomplish this execution in a wide range of network setups, DIP utilizes a cross breed approach of randomized checking and tree-based coordinated quests. By progressively choosing which of the two algorithms to utilize, DIP outflanks both as far as transmissions and speed. Reenactment and testbed tests demonstrate that DIP sends 20-60% less parcels than existing conventions and can be 200% quicker, while just requiring O(log(log(T))) extra state per data thing. To help network programming, we present Deluge, a solid data spread convention for proliferating extensive data objects from at least one source nodes to numerous different nodes over a multihop, At scale, the convention uncovered fascinating proliferation elements just indicated by past scattering work. A basic model is likewise determined which depicts the breaking points of data engendering in wireless networks. At last, we contend that the rates got for scattering are naturally lower than that for single way spread. It seems hard to altogether enhance the rate gotten by Deluge and we recognize building up a tight lower bound as an open issue.

Keywords: Distributed Data Discovery and Dissemination, Wireless Sensor Networks, DiDrip, Network Owners.

I. Introduction

Wireless sensor network comprise of various sensor nodes that are profoundly appropriated network of all little and light weighted nodes that are spread over the framework in vast numbers by the estimation of physical parameters, for example, temperature, ecological checking, combat zone observation, weight, relative mugginess hostile to fear based oppression and other hazardous situations. Every node of the sensor network comprises of three subsystem i.e. sensor framework that sense the earth, process subsystem that performs local calculation on the detected data, and correspondence framework is in charge of message trade with neighboring sensor node. Wireless Sensor Networks have an extensive variety of uses, going from perception situations, military zones, delicate establishments and remote data collection and investigation. The major essential task in sensor network is data spread. Inside the sensor network, inquiries or data are steered. Whatever other node that is keen on the information or base station should be conveyed by sensor node for accumulation of detecting data. Working of source is to produce the data and occasion might be performed once data to accord. The working of sink is that, a node that is keen on an occasion and it will ask for a few data. DiDrip comprises of four stages, initial one is framework instatement stage, second one is client joining stage, third one is packet pre-preparing stage lastly fourth one is parcel confirmation stage. For our essential convention, in framework instatement stage, the network proprietor makes its open and individual keys and after that hundreds people in general parameters on each node before the network organization. The second stage is client joining stage, a client gets the scattering benefits through enrolling to the network proprietor. The third stage is parcel preprocessing stage, if a client enters to the network and needs to spread a few data things, he/she can need to build the data

scattering packets and after that send them to the nodes. The fourth stage is packet confirmation stage, a node checks each gotten parcel if the outcome is sure, and it refreshes the data as indicated by the got packet. In incorporated data dispersal process, the data to the sensor nodes can be engendered by just the base station; this does not bolster rising idea of multi proprietor multi-client WSNs. These conventions were not planned in view of security and thus foes can without much of a stretch dispatch assaults to mischief to the network, where as in conveyed process data can be dispersed by numerous proprietors and various clients. In the event of an incorporated engineering of sensor network on the off chance that the focal node or the base station falls flat, the whole network will crumple, anyway the unwavering quality of the sensor network can be expanded by utilizing appropriated control design. Appropriated process is embraced in WSNs for the accompanying reasons.

II. Related Work

The paper [1] proposed by Daojing He et al, is a code dispersal convention reasonable for a circulated domain. In this convention various network clients are permitted to disperse data things to sensor node without relying upon base station. This appropriated code dispersal convention incorporates a network proprietor, network clients and sensor nodes. After the enrollment network clients can spread data. Network proprietors are genuine endorsers though the clients are intermediary underwriters. A cryptographic strategy called intermediary signature by warrant is utilized This dispersal convention is refusal of administration assault safe. The paper [2] proposed by Daojing He et al. is a secure and dispersed code spread convention named SDRP. In this convention diverse clients have distinctive benefits. Benefits are allocated by the network proprietor. It utilizes a system called personality based cryptography. For secure dispersed data spread Certificate Based Approach (CBA) is pursued. Every client will have an open private-key combine. Client signs the code picture utilizing ECDSA algorithm before scattering. DIDRIP [3] proposed by Daojing He, Sammy Chan, Mohsen Guizani and Haomiao Yang is a secure and circulated data scattering convention. DIDRIP involves a network proprietor, clients and sensor nodes. Network proprietor has an open private key match. Each network client gets an authentication subsequent to enrolling with the network proprietor. Clients additionally have an open private key combine and scattering benefit. At the point when client needs to spread data he will develop the parcel and signs with his private key. Client testament is additionally transmitted alongside affirmation packet. This declaration is utilized by the nodes for verification. There are some effectiveness issues with this DIDRIP. It isn't efficient in correspondence since the endorsement should be transmitted with the ad parcel. Likewise signature check is costly in light of the fact that testament ought to dependably be verified first. A few conventions guarantee Authenticity and Integrity. Classification of data is an imperative perspective however it isn't guaranteed by any current circulated data scattering convention. In[3] Ensuring that each sensor node has a similar code variant is trying in dynamic,unreliable multi-bounce sensor networks. At the point when nodes have distinctive code forms, the network may not act as planned, sitting around idly and energy. We propose and assess DHV[5], an efficient code consistency support convention to guarantee that each node in a network will in the long run have a similar code. DHV depends on the basic perception that if two code variants are unique, their comparing form numbers regularly vary in just a couple of minimum huge bits of their paired portrayal. DHV enables nodes to deliberately choose and transmit just fundamental piece level data to recognize a more up to date code form in the network.DHV can distinguish and recognize variant contrasts in O (1) messages and inertness contrasted with the logarithmic size of current conventions. Reenactments and trials on a genuine MicaZ test bed demonstrate that DHV lessens the quantity of messages by half, meets in a fraction of the time, and decreases the quantity of bits transmitted by 40-60% contrasted with DIP, the state-ofthe-craftsmanship convention. In[4] When a sender sends a packet to a recipient, beneficiary will keep the parcel in a support. In the event that a cradle is full, the packet is disposed of and henceforth causes an issue. To defeat an issue a strategy is utilized called TESLA. This procedure is utilized by the sender. A parcel is sent utilizing a sender MAC incentive to the packet to the recipient and collector keep it in support. On the off chance that the sender encases the parcel, beneficiary will validate it with the goal that no misfortune is there. Along these lines both sender and collector get

conveyed. Multicast innovation [4] application has been generally used in broadband web. Source confirmation is a standout amongst the most requirements for some multicast applications exchanging constant data, for example, stream video and online news. Since multicast current administrations gave to the gathering individuals are changed powerfully, data exchanging by a gathering part isn't utilized by the beneficiary. So as to confirm the character of the sender who sent the parcel and to ensure that the data have not been altered, an improved source validation plot has been proposed to exchange the verification data not to the nearby packet.

III. Methodology

Secure DiDrip:

Each node in the Wireless Sensor Network should receive a replica of disseminated data. For this the Trickle algorithm is used, which is used by more number of dissemination protocols. So as to ensure the freshness of data version variety is used. Every data item is identified by the tuple (key, version, and data).Since detector nodes are resource restricted devices a lightweight weight block cipher encryption rule is used for encrypting the disseminated data. The algorithm used is based on chaotic maps and genetic operations that are appropriate for wireless environment. The projected SecDiDrip consists of four phases, First phase is system initialization, second phase is user registration, third phase is packet creation and finally fourth phase is packet verification. In system initialization part, the network owner creates its public and private keys and encoding key, and then loads the general public parameters on every node before the network deployment. Within the user registration phase, a user registers with the network owner to induce dissemination privilege. In packet creation part, if a registered user desires to diffuse some information things, he/she can need to construct the data dissemination packets, encrypt the packet then send them to the nodes. Within the packet verification phase, a node verifies every received packet. If verification passes, it updates the data according to the received packet. In the following, every part is described in detail.

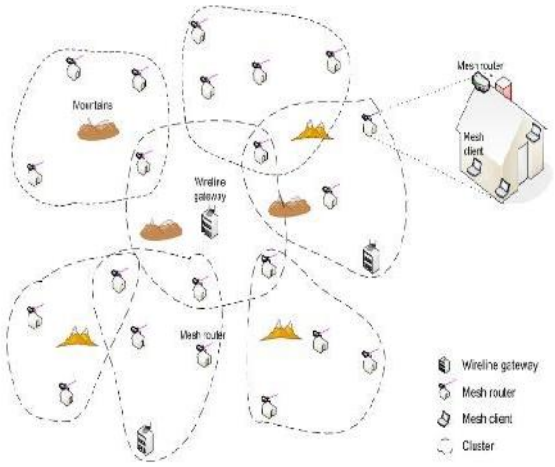


Figure: Decentralized Wireless Sensor Network

System Initialization:

At the initialization stage the base station runs a code to derive personal key X and corresponding personal key y. Afterthat the connected public parameters are preloaded in every node of the network. An encoding key's additionally established bythe base station. For encoding key establishment an elliptic curve over prime field is used. This key along with Userid and privilege level of each user is pre loaded in each node.

Registration phase:

In the user registration phase user with the identity has to register with the bases station so as to get privilege level. User requests for the privilege level by submitting 3tuple to the network owner, where the privilege level of user is that the public key of the user. User chooses the personal key from field over q and computes the general public key when receiving the request the network owner uses to sign the tuple with its personal key. This tuple is send to every sensor node.

Packet Creation Phase:

After completing the registration phase a user will disseminates data items to nodes. Suppose that a user say UID wants to circular rise n data items I = 1, 2, n. User initial needs to encode the information thing using the light-weight encoding algorithm. The algorithm projected is used for encoding. For that a Pseudo random bit sequence is to be generated at first. This sequence is used in encoding method and is generated using chaotic functions. Merkle hash tree

method is used for the construction of data packet. Merkle hash tree is constructed as follows. At first all the data things are treated because the leaves of the tree. The hash value of two child nodes is computed and concatenated to make every internal node. This process is sustained till the root node root is formed, resulting in a Merkle hash tree when the development of tree the root of the tree is signed by the user using his private key. Then transmits the ad packet P0 comprising user, root subsequently, user disseminates every data item along with the appropriate internal nodes for verification purpose.

Packet Verification Phase:

When a sensing element node, say, receives a packet either from a certified user or from its one-hop neighbors, it first checks the packet's key field. If this can be a poster packet P0, node j uses the to choose up the dissemination privilege. Then examine the

lawfulness of. If the result's positive, node Sj uses the public key y of the network owner to run an ECDSA verify operation to attest the signature. If yes, node stores enclosed within the ad packet; otherwise, node merely discards the packet. Otherwise, it's an information packet Pi, wherever I = 1, 2, n. Node executes the subsequent procedure: Node S checks the believability and integrity of Pi through the already verified root node received within the same spherical. If the result's positive and also the version variety is new, node S then decipher the information (decryption algorithmic program is same as encryption algorithm), updates the information known by the key hold on in Pi, otherwise, Pi is discarded.

IV. Energy Consumption of Sensor Node

The sensor nodes operate in the three modes of sensing, computing and communications, and all of which consume energy. Of the three modes, maximum energy is expended for the communications process. The sensing unit is entrusted with the responsibility to detect the physical characteristics of the environment and has an energy consumption that varies with the hardware nature and applications. However, sensing energy represents a meagre percentage of the entire energy consumption within the entire WSN. In comparison, computations energy is much more. The communication unit consists of a short-range RF circuit which performs the transmission and reception tasks.

Communication energy contributes to data forwarding and it is determined with the transmission range that increases with the signal propagation in an exponential way. The energy consumption model includes the five states: *Acquisition, Transmission, Reception, Listen and Sleep* [2].

Since the sensor nodes can be in any of three main operations of sensing, computations and communications, each of them could be in different states depending on the component nature. Accordingly different levels of energy are expended in each of them.

States of the energy consumption model.

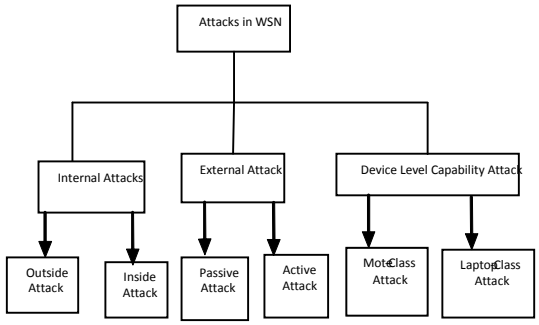
(i) **Acquisition**: The acquisition state includes sensing, A/D conversion, pre-processing and eventually storage of these data.

(ii) **Transmission**: The transmission state includes processing, packet forming, encoding, framing, queuing and base band adapting to RF circuits.

(iii) **Reception**: This state is responsible for low noise amplification, down converter oscillator, filtering, detection, decoding, error detection, address checking and random reception.

(iv) **Listen**: The listen state is similar to reception and involves the processes of low noise amplification, down convertor oscillator, filtering and terminates at detection.

Sleep: The sleep state expends least energy as compared to the other states.



V. ATTACKS ON WSN

A. Internal Attacks

These are primarily done as a result of the bargained hubs. These traded off hubs ceaselessly look to upset or parallelize the system. In light of sort of action performed by assailant, it tends to be additionally named: Outside Attack-in which, an aggressor can supplant/present new pernicious hub from outside. Inside Attack-in which, an aggressor can catch any hub; reconstruct it, to go about as vindictive hub.

B. External Attacks

Fig. 2 Attack characterizations in WSN

In these assaults, the assailant hub isn't generally an approved take part of SN. Rely upon the direct of aggressor hub, it could be arranged as:

• Passive Attack-it include listening stealthily on or checking bundles swapped inside a WSN. It includes just unapproved tuning in to the steering bundles.

By and large, encryption is the standard answer for shield against these assaults.

• Active Attack-it incorporate couple of changes of the information steam or the creation of a wrong stream. Likewise, it brings about upsetting system functionalities by presenting DOS assaults, Jamming assaults and Power Exhaustion.

C. Device Level Capability Attack

This class of assaults is ordered rely upon the capacity of the gadget that is being utilized for assaulting. An assailant may assault the WSN either utilizing a sensor gadget (Sensor Level) or all the more amazing PC gadget (Laptop Level). A foe can exceedingly harm the framework on the off chance that he/she utilizes Laptop Class assault having all the more ground-breaking calculation, stockpiling and battery life. Next to the previously mentioned arrangements, an assailant may use at least one of the ensuing assault systems, for example,

D. Eavesdropping

In which an assailant quietly tune in to media for dispatch in the midst of two gatherings and don't changes the information. It's a uninvolved strategy.

E. Radio sticking

In this assault, the aggressor endeavors to upset the correspondence by sending few radio waves at the comparable recurrence bringing about obstruction or crashes of parcels over system. Sticking can be irregular or consistent rely upon the ideal opportunity for which arrange is kept stuck.

F. Message's infusion

In this the aggressor transmits numerous false messages over system in lieu of undermining the bundle information or to just fumes arrange.

G. Message's replication

In this the aggressors catch and resend a similar bundle commonly to same or distinctive sensor and at various occasions in arrangement to make collector silly.

H. Node bargain (Destruction or robbery) This incorporates physical catching of a hub in arrangement to disturb organize by breaking the correspondence way or reconstructing a hub so it goes about as a government operative in system.

I. Denial of Service (DoS)

In this the assailant will consistently sends parcel in succession to upset administrations or battery control by utilizing pernicious hubs. This is a functioning sort of assault.

J. HELLO Flooding

We realize that HELLO message is utilized for finding neighbors. In this type of assault, the aggressor utilizes all the more amazing hubs to send HELLO messages to far away sensor hubs so they believe that the malevolent hub is their neighbor and they will exchange future parcels to it.

K. Black Hole Attack

In this assault a hub attempts to end up beneficiary of bundles of neighboring hubs by adjusting their steering table and it will never forward the parcels to address goal.

L. Selective Forwarding (Gray Hole Attack) in this assault, the aggressor will embed hub of malevolent in the n/w which endeavors to change the directing and catch information simply like dark

opening assault however dissimilar to it will specifically forward information (not all) thus hard to distinguish.

M. Wormhole Attack

This sort of assault is finished with something like two vindictive hubs which have high data transmission between them either wired or remotely. These malevolent hubs will indicate other ordinary hubs that they give the shorter way to the objective regardless of whether they are lying far away in the system. Along these lines, the hub will forward information to the vindictive hub that can be caught by aggressor effortlessly.

N. Sinkhole Attack

In this assault the malignant hub dwell close to the BS and it attempts to fanciful to be nearest hub to the BS with the goal that other encompassing common hub will change themselves and forward information to the noxious hub.

C. Sybil Attack

In this attack the adversary tries to have several individualities to different nodes and thus can be in more than one place at single time. Here it tries to be voted as the cluster head. A Sybil attacks is extensive risk to Geographic Routing Protocols.

D. Infinite Loops-

In this attack two or more malicious node tries to circulate packets infinitely in the n/w in sequence to exhaust power of the network.

E. Message Alteration

In this attack the node of malicious will capture and modify packets on the network. It can add false data or delete data so that packet will become corrupted.

F. Sleep deprivation torture

In this attack, the malicious node will prevent a node from sleeping by sending messages to it or asks for calculation. This is complete so that the node will consume its power quickly [4].

VI. Proposed Work

Proposed work include distributed dissemination of data instead of using centralized approach. The distributed dissemination protocol used is DiDrip[2]. It consists of 4 phases, System Initialization, User joining, Packet preprocessing and Packet verification For our basic protocol[7], in system initialization the network owner creates its public and private keys, and so masses the general public parameters on every node before the network. Within the user joining section, a user gets the dissemination privilege through registering to the network owner. In packet preprocessing section, if a user enters the network and needs to circularize some knowledge things, he/she can have to construct the packets andsend them to the nodes. Within the packet verification section, a node verifies every received packet.

VII. Conclusion and Future Work

In this paper, we identified the security vulnerabilities in data discovery and dissemination used in WSNs, Therefore, in this paper, a secure and distributed data discovery and dissemination protocol named DiDrip has been proposed. Analyzing the security of DiDrip, this paper has also reported the evaluation results of DiDrip in an experimental network of resource-limited sensor nodes, which 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.

Thus, in the future work, we will consider how to ensure data confidentiality in the design of secure and distributed data discovery and dissemination protocols

References

[1]. 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.

[2]. 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.

[3]. 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.

[4]. 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.

[5]. 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.

[6]. 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.

[7]. 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–

[8]. JoppeW.Bos, J. Alex Halderman , Nadia Heninger , Jonathan Moore, Michael Naehrig, and Eric Wustrow, “Elliptic Curve Cryptography in Practice”

[9]. 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.

[10]. Geoss. [Online]. Available: http://www.epa.gov/geoss/

Mr. B.Manikumar , Pursuing M.Tech (CSE) from Avanthi Institute of Engineering and Technology, Vizianagaram, A.P. Received his B.Tech from Visakha institute of engineering and technology , Visakhapatnam . He actively participated in various workshops, and seminars and presented papers related to informationt echnology. His area of interests are cloud computing, Networking and Network security.

Mr. Kesavarao Seerapu , M.Tech(CSE) is working as a Assistant Professor, Department of CSE Avanthi Institute of Engineering &Technology, Vizianagaram, AP, INDIA. He is an M.Tech post graduate in Computer Science &Engg. From JNTU Kakinada. He attendedseveral seminars and workshops. His goal in his life is to do PhD and research on advanced topics and serve for the mother country.