# Secure And Efficient Didrip Protocol For Improving Performance Of The Wireless Sensor Networks

**Dr. K.Suresh Babu[1], Kasthuri Yashwanth[2]**
[1]Senior Assistant Professor, Dept of CSE
[2]Dept of CSE
[1, 2] School of Information Technology JNTUH, Village KPHB,
Mandal Kukatpally, District RangaReddy, Telangana, India

***Abstract-*** *A Wireless sensor network (WSN) may be a network together with sensor nodes that connected through wireless media. When the deployment of a WSN some common variables such as sensing interval, data sending interval or small programs stored in each node of the network might have to be updated or modified. Since sensor nodes are distributed in ad hoc fashion manual updating is not always attainable. Therefore we tend to usedata dissemination protocols to alter the sensor configuration parameters. Two main drawbacks are suffered by existing data discovery and dissemination protocols. First, they are based on the centralized approach; during this approach only base station will disseminate data items. Such an approach suffers from single purpose of failure. Second, most protocols assume that working environment is safe, therefore attackers will easily harm network. In Wirelesssensor Network, the security and confidentiality ofdata is important. This paperproposes a secure and distributed data dissemination protocol named Secure DiDrip. It allows numerous authorized network users to honestly disseminate data items to the sensor nodes. Secure -Drip enhances ensures the confidentiality of disseminated data therefore enhances security.*

***Keywords***- Wireless Sensor Network, Data Dissemination, Confidentiality, Data Encryption;

## I. INTRODUCTION

Wireless sensor Networks (WSNs) are attracting nice interest during a very wide range of applications related to observance and control of environmental or physical conditions, like business observation and military operations. Once a WSN is deployed among the field, it should be necessary to update the place in programs or hold on parameters in device nodes show in figure one. This may be achieved by dissemination services that ensure new programs or parameter values to be propagated throughout the WSN therefore all nodes have identical copy. Normally, a new program is of the order of kilobytes whereas a parameter is entirely few bytes long. As a result of such a massive difference between their sizes, the planning issues of their dissemination protocols are dissimilar. As a result, two varieties of dissemination protocols are developed among the literature. Code dissemination we tend to tend to additionally cited as data dissemination or reprogramming protocols are developed to efficiently disperse long messages into a network, enabling complete system reprogramming. On the other hand, data discovery and dissemination protocols are accustomed distribute short messages, like many two-byte configuration parameters, among a Wireless device Networks. Common uses of this sort of protocols include injecting little programs, commands, queries, and configuration parameters. Recently, many data discovery and dissemination protocols are projected. Among them, Drip, DIP and DHV are most traditional and enclosed in little OS distributions. Though, our data, all existing data discovery and dissemination protocols only address reliable data transmission, however give no security mechanism. Certainly, usually this can be often a significant issue that has to be addressed. Otherwise, adversaries would possibly, as an example, distribute viral or false information to cripple a Wireless Sensor Networks deployed within the battlefield.

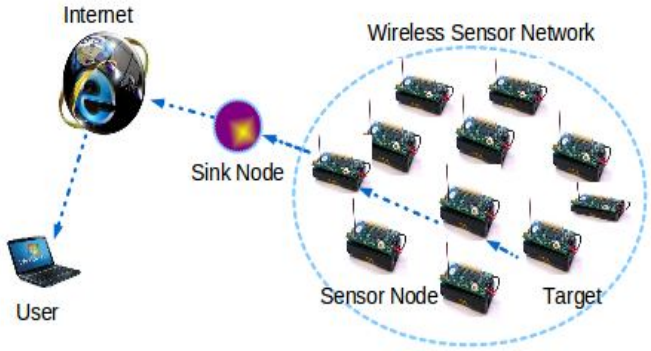



Figure 1: Architecture of Wireless Sensor Network

In an endeavor to construct these protocols secure, this paper has the subsequent main contributions: 1) we tend to tend to initial investigates the protection problems in data discovery and dissemination methodology of WSNs and entails that the dearth of authentication of the disseminated data introduces an exposure to the update of arbitrary data in

Wireless device Networks. 2) We tend to tend to then develop a secure, light-weight, and Denial-of Service (DoS)-resistant data discovery and dissemination protocol named Secure DiDrip for WSNs that may be a secure extension of Drip. To realize DoS-attack resilience and allow immediate verification of any received packets, Secure Di-Drip depends on a signed Merkle hash tree. This manner the lowest station of a Wireless device Networks should sign only the basis of this tree. Also, Secure DiDrip will tolerate the compromise of some detector nodes. To further improve the security and efficiency; some further mechanisms like the message specific puzzle approach are incorporated into the planning of Secure DiDrip. 3) We tend to tend as well implement the projected protocol in networks. Experimental results demonstrate its high efficiency in follow. To the most effective of our data, generally this will be usually together the primary implemented secure data discovery and dissemination protocol for Wireless sensor Networks.

## II. RELATED WORK

The paper projected by Daojing He et al, may be a code dissemination protocol appropriate for a distributed environment. During this protocol multiple network users' area unit allowed to disseminate data things to sensor node without depending on base station. This distributed code dissemination protocol includes a network owner, network users and sensor nodes. When the registration network users will disseminate data Network owners are actual signers whereas the users are proxy signers. A cryptographic technique referred to as proxy signature by warrant is used this dissemination protocol is denial of Service attack resistant. The paper planned by Daojing He et al. could be a secure and distributed code dissemination protocol named SDRP. During this protocol completely different users have different privileges. Privileges are assigned by the network owner. It uses a way referred to as identity-based cryptography. For secure distributed data dissemination Certificate Based Approach (CBA) is followed. Every user can have a public-private-key combine. User signs the code image using ECDSA algorithm before dissemination. DIDRIP planned by Daojing He, Sammy Chan, Mohsen Guizani and Haomiao principle could be a secure and distributed data dissemination protocol. DIDRIP includes a network owner, users and sensor nodes. Network owner includes a public-private key combine. Every network user gets a certificate when registering with the network owner. Users additionally have a public non-public key combine and dissemination privilege. Once user has to disseminate data he can construct the packet and signs together with his non-public key. User certificate is additionally transmitted together with acknowledgement packet. This certificate is employed by the nodes for authentication. There are some potency issues with this DIDRIP. It is not efficient in communication since the certificate need to be transmitted with the advertisement packet. Additionally signature verification is expensive as a result of certificate should always be etched initial. Some protocols ensure authenticity and Integrity. Confidentiality of data is an important aspect however it is not ensured by any existing distributed data dissemination protocol.

## III. DIDRIP PROTOCOL

The need of DIDRIPDistributed Data Discovery and Dissemination Protocols is not completely new, however previous work did not address this would like. We tend to study the useful necessities of such protocols, and set their design objectives. Also, we tend to establish the security vulnerabilities in previously projected protocols.2) based on the design objectives, we tend to propose DiDrip. It is the primary distributed information discovery and dissemination protocol that allows network owners and authorized users to broadcast information things into WSNs without looking forward to the base station. Moreover, our extensive analysis demonstrates that DiDrip satisfies the protection requirements of the protocols of its kind. Particularly, we tend to apply the demonstrable security technique to formally prove the authenticity and integrity of the disseminated data items in DiDrip. 3) We tend to demonstrate the efficiency of DiDrip in observe by implementing it in an experimental WSN with resource-limited sensor nodes. This is additionally the primary implementation of a secure and distributed data discovery and dissemination protocol. In addition, distributed information discovery and dissemination is a more and more relevant matter in WSNs, particularly within the aborting context of shared sensor networks, wherever Sensing/communication infrastructures from multiple owners are going to be shared by applications from multiple users. As an example, massive scale sensor networks are built in recent these networks are owned by multiple owners and utilized by numerous authorized third-party users. Moreover, it is expected that network owners and totally different users might have different privileges of dissemination.

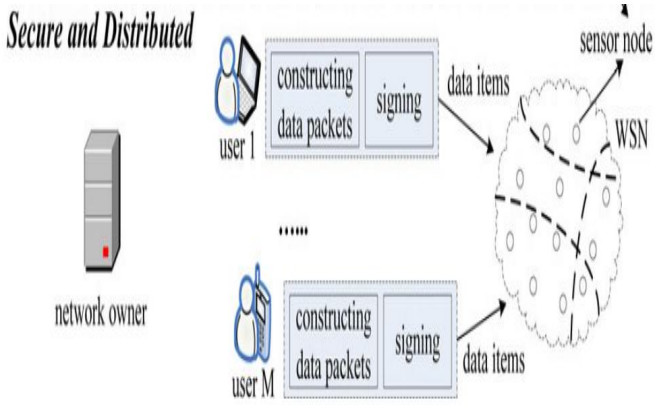



Figure 2: Architecture of Decentralized Wireless Sensor Network

System Initialization Phase: In System initialization stage the base station runs a code to derive personal key X and corresponding personal key y. subsequently the connected public parameters are preloaded in every node of the network. A cryptography key's additionally established by the base station. For cryptography key establishment an elliptic curve over prime field is used. This key at the aspect of User id and privilege level of each user is pre loaded in each node.

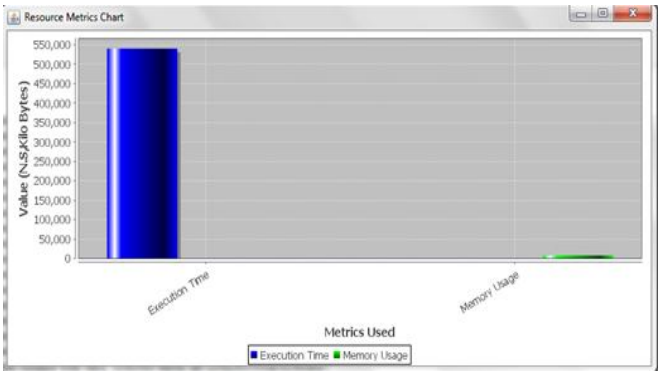
Registration Phase: in the user registration section user with the identity should register with the bases station soon get concession level user requests for the privilege level by submitting 3-tuple to the network owner, where the privilege level of user is that the public key of the user. User chooses the private key from field over Q and computes the general public key once receiving the request the network owner uses to sign the tuple with its personal key this tuple is send to each sensor node.

Packet Creation Phase: after completing the registration section a user will disseminates data things to nodes. Suppose that a user say UID has to circular rise n data things I = 1, 2,…,n. User initial should write the data issue using the light-weight cryptography algorithm. The algorithm projected is used for cryptography. For that a Pseudo random bit sequence is to be generated initially. This sequence is used in cryptography technique and is generated using chaotic functions. Merkle hash tree technique is used for the development of data packet. Merkle hash tree is made as follows. Initially all the data things are treated as results of the leaves of the tree. The hash value of two child nodes is computed and concatenated to make every internal node. This technique is sustained until the basis node root is created, resulting in a Merkle hash tree once the development of tree the basis of the tree is signed by the user using his non-public key. Then transmits the ad packet P0 comprising user, root after, user disseminates every data item at the aspect of the suitable internal nodes for verification purpose.

Packet Verification Phase: In Packet Verification phase once a device node, say, receives a packet either from a certified user or from its one-hop neighbors, it initial checks the packet's key field. If this can be a commercial packet P0, node j uses to choose the dissemination privilege. Then examine the standard of. If the result's positive, node Sj uses the non-private key y of the network owner to run associate Elliptic Curve Digital Signature algorithm or ECDSA verify operation to attest the signature. If yes, node stores swallowed among the ad packet; otherwise, node merely discards the packet. Otherwise, it is a data packet Pi, wherever I = 1,2,…, n. Node executes the next procedure: Node S checks the standard and integrity of Pi through the already verified root node received among an equivalent spherical. If the result is positive and together the version choice is new, node S then deciphers the data (decryption algorithm is same as cryptography algorithm), updates the data well-
Known by the key hold on in Pi, otherwise, and Pi is discarded.

## IV. EXPERIMENTAL RESULTS

In our experiments, network owner is register the any number of users with privileges after successfully registering the users and issue the keys for the registered users after keys assign to the users multiple nodes are generated in the network simulation screen and registered users are join in these network after joining in the network users are disseminate some data in specified commands with in privileges assign by the users the data is disseminated in encryption format so these process to increasing the lifetime of the network and disseminate the data in secure format by using hash tree method. In the below chart we can observe that difference between the length of Execution Time and Memory Usage




We can observe thatResource Metrics chart Execution Time length is higher than Memory Usage length. The difference

will be shown in the sense of Value in (Nanoseconds, Kilobytes). So we can consider that the advantage of decentralized wireless sensor network. Through our implementation we can improve the lifetime of the network and disseminate the data in secureformat at lower cost then compare to current protocols.

## V. CONCLUSION

Security is that the need of the hour in data dissemination. In Wireless Sensor Network as attackers will send fake data into the network to cause false updates or denial of service attacks. Additionally as a result of the open nature of wireless channels, messages will be simply intercepted. Therefore secure protocol that ensues confidentiality, integrity, authenticity and freshness of data is shall for data dissemination. Secure-Didrip may be a secure and distributed data dissemination protocol that may be used for the secure and efficient dissemination of data in wireless sensor networks.

## REFERENCES

[1] Daojing He, Chun Chen, Sammy Chan and Jiajun Bu, “DiCode: DoS-Resistant and Distributed Code Dissemination in Wireless Sensor Networks”, IEEE Transaction on Wireless communication, VOL. 11, NO.5, MAY 2012.

[2] S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, “A novel ultrathin elevated channel low-temperature poly-Si TFT,” IEEE Electron Device Lett., vol. 20, pp. 569–571, Nov. 1999.

[3] Daojing He, Member, IEEE, Sammy Chan, Member, IEEE, Mohsen Guizani, Fellow, IEEE, Haomiao Yang, Member, IEEE, and Boyang Zhou "Secure and Distributed Data Discovery and Dissemination in Wireless Sensor Networks".

[4] Mohammad A. Matin, Wireless Sensor Networks: Technology and Protocols: Published by InTech, Croatia, ISBN 978-953-51-0735-4, 2012.

[5] Salvatore La Malfa, Wireless Sensor Networks, 2010.

[6] Jisha Mary Jose, Jomina John, “Data dissemination protocols in wireless sensor networks-a survey”, IJARCCE, March 2014.

[7] R.Merkle, “Protocols for public key cryptosystems,” in Proc. IEEE Security Privacy, 1980, pp. 122–134.

[8] Jisha Mary Jose, "Security Issues During Data Dissemination in Wireless Sensor Networks", International Journal of Advanced Research Trends in Engineering and Technology, March 2015.

[9] Hong-Ning Dai, Qiu Wang, Dong Li, and Raymond Chi WingWong, “On Eavesdropping Attacks in Wireless Sensor Networks with Directional Antennas”, International Journal of Distributed Sensor Networks Volume 2013.

[10] Daojing He, Sammy Chan, Mohsen Guizani, "Small Data Dissemination for Wireless Sensor Networks: The security Aspect” IEEE. 2014

[11] Kamanashis Biswas, Vallipuram Muthukkumarasamy, Kalvinder Singh, An Encryption Scheme Using Chaotic Map and Genetic Operations for Wireless Sensor Networks, ARTICLE in IEEE SENSORS JOURNAL·DECEMBER 2014.

[12] 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.

[13] P. Levis et al, "Trickle: A Self-Regulating Algorithm for Code Maintenance and Propagation in Wireless Sensor Networks", Proc. NSDI, 2004.

[14] T. Ho and D. Lun. Network Coding: An Introduction. Cambridge University Press, 2008.

[15] 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.