IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-5, Issue-6 E-ISSN: 2347-2693

# A Lightweight and Reliable Routing Approach for in-Network Aggregation in Wireless Sensor Networks

**G. Vinitha[1*], K. Bhuvaneshwari[2]**

[1*]Dept. of Computer Science, ARJ College of Engineering and Technology, Mannargudi, India
[2]Dept. of Computer Science, ARJ College of Engineering and Technology, Mannargudi, India

**Corresponding Author: vinithacsebe@gmail.com*

**Available online at: www.ijcseonline.org**

Received: 25/May/2017, Revised: 02/Jun/2017, Accepted: 20/Jun/2017, Published: 30/Jun/2017

***Abstract*—** A focal issue in sensor network security is that sensors are defenseless to physical catch attacks. Once a sensor is traded off, the foe can without much of a stretch dispatch clone attacks by reproducing the bargained node, dispersing the clones all through the network, and beginning an assortment of insider attacks. Past conflicts with clone attacks experience the ill effects of either a high correspondence/stockpiling overhead or a poor discovery precision. Wireless Sensor Networks (WSNs) offer an incredible chance to screen conditions, and have a great deal of fascinating applications, some of which are very touchy in nature and require full verification secured condition. The security components utilized for wired networks can't be specifically utilized as a part of sensor networks as there is no user-controlling of every individual node, wireless condition, and all the more significantly, rare vitality assets. In this composition, we address a portion of the extraordinary security dangers and attacks in WSNs. In our proposed work, a novel clone detection framework, called CSI to overcome the previous clone detection problems. We introduce two algorithms are CSI-1 and CSI-2.The CSI-1 (Ordinary Compressed Sensing-Based Approach) algorithm used to construct an aggregation tree. The CSI- 2 (Random Projection-Based Approach) is used to reduce the communication cost. Our proposed CSI method not only achieves lowest communication cost but also manage the network traffic evenly spread over sensor nodes. The presentation and security of CSI will be demonstrated feasibility of clone detection.

***Keywords*—** WSN, Cloning Attack, Man-in-the-Middle Attack, Zero Knowledge Protocol.

## I. INTRODUCTION

In sensor networks, enemies may effortlessly catch and bargain sensors and send boundless number of clones of the traded off nodes. Since these clones have genuine access to the network (authentic IDs, keys, other security accreditations, and so on.), they can take an interest in the network operations in an indistinguishable path from an honest to goodness node, and subsequently dispatch a substantial assortment of insider attacks, or even assume control over the network. On the off chance that these clones are left undetected, the network is unshielded to assailants and in this way to a great degree helpless. In this way, clone aggressors are seriously dangerous, and viable and productive answers for clone attack location are expected to restrain their harm. In any case, distinguishing clone attacks is not inconsequential by any means. The crucial test originates from the way that the reproductions claim all the security data (ID, keys, codes, and so forth.) of the first bargained sensor. Along these lines, they can pass all the personality/security check and escape from being recognized from a true blue sensor. Also, a "shrewd" clone may attempt to escape being recognized definitely. Moreover, clones may conspire to cheat the network chairman into trusting that they are genuine. Take note of that a foe may disperse clone nodes anyplace in the network. Along these lines confined discovery plans don't work adequately. Propels in innovation have made it conceivable to create sensor nodes which are conservative and economical. They are mounted with an assortment of sensors and are wireless empowered. When sensor nodes have been sent, there will be negligible manual intercession and observing. In any case, when nodes are sent in an antagonistic domain and there is no manual observing, it makes a security concern. Nodes might be subjected to different physical attacks. The network must have the capacity to self-sufficiently recognize, endure, or potentially maintain a strategic distance from these attacks. One vital physical attack is the presentation of cloned nodes into the network. At the point when item equipment and working frameworks are utilized, it is simple for an enemy to catch real nodes, make clones by replicating the cryptographic data, and sending these clones once more into the network.

These clones may even be specifically reinvented to subvert the network. Singular sensor node contains a light weight processor, shoddy equipment parts, less memory. On account

of these limitations, universally useful security protocols are not really suitable. Open key cryptography depends on RSA approach. The vitality utilization and computational idleness makes RSA improper for sensor network applications. Security calculations that are composed particularly for sensor networks are observed to be more reasonable.

The objective of this composition is to build up a security demonstrate for wireless sensor networks. We propose a strategy for recognizing the traded off/cloned nodes and furthermore confirming the realness of sender sensor nodes in wireless sensor network with the assistance of zero knowledge protocol. The proposed strategy joins the past framework nature and actualizes the proposed technique to validate the cloned nodes.

## II. RELATED WORK

A direct answer for safeguard against clone attacks is to give the base station a chance to gather the area data (e.g. area, neighbor list, and so forth.) from every sensor and screen the network in a brought together way. This approach experiences high correspondence overhead by asking for repetitive data from the network. Facilitate, a "brilliant" clone may report the area of the first node, making the base station flop in distinguishing the replicaIn, Y. Zeng et al. propose for one-jump networks that the base station (BS) can store the special flag trademark for every gadget, and consequently gadget cloning can be recognized in like manner. In any case, in a multi-jump sensor network, it is illogical for BS to track the flag attributes of sensors multi-bounces away. In limited voting/misconduct identification plans, nodes inside an area concur/vote on the authenticity of a given node in light of their nearby perceptions. All things considered, these plans are not equipped for identifying clones with ordinary conduct, and may fall flat when different clones in closeness connive. Besides, restricted voting/misconduct location plots intrinsically do not have the capacity to distinguish dispersed clones that may show up at wherever in the network.

### *A. Important Attacks in WSN*

In spite of the fact that there are different attacks in Wireless Sensor Networks, yet certain dynamic attacks, that can be recognized with our proposed model are as per the following:

1. Clone Attack

In clone attack, a foe may catch a sensor node and duplicate the crytographic data to another node known as cloned node. At that point this cloned sensor node can be introduced to catch the data of the network. The foe can likewise infuse false data, or control the data going through cloned nodes. Consistent physical checking of nodes is unrealistic to recognize potential altering and cloning. Accordingly solid and quick plans for location is important to battle these attacks.

2. Man in the Middle Attack

The Man-In-The-Middle attack (MITM) is a type of dynamic listening stealthily in which the attacker makes autonomous associations with the casualties and transfers messages between them, making them trust that they are talking specifically to each other over a private association. The attacker will have the capacity to catch all messages trading between the two casualties and infuse new ones.

3. Replay Attack

A replay attack is a type of network attack in which a legitimate information transmission is noxiously or deceitfully rehashed or postponed. This is done either by the originator or by enemy who captures the information and retransmits it. This sort of attack can without much of a stretch overrule encryption.

### *B. Zero Knowledge Protocol*

Zero-knowledge protocol permit recognizable proof, key trade and other essential cryptographic operations to be executed without uncovering any mystery data amid the discussion and with littler computational prerequisites in contrast with open key protocols. Along these lines ZKP is by all accounts exceptionally appealing for asset obliged gadgets. ZKP enables one gathering to demonstrate its knowledge of a mystery to another gathering while never uncovering the mystery. ZKP is an intelligent evidence framework which includes a prover, P and verifier, V. The part of the prover is to persuade the verifier of some mystery through a progression of correspondences. Every correspondence includes a test, or question, from the verifier and a reaction, or reply, from the prover. ZKP based protocols require less data transmission, less computational power, and less memory contrasted with other validation strategies and in this manner is by all accounts reasonable for WSN.

### *C. Basic Mechanism of Zero Knowledge Protocol*

The utilization and implementation of ZKP in frameworks and gadgets that have limited computational asset are depicted. The prover P and the verifier V may utilize some numeric esteem, alluded as the mystery number of the prover P. Ordinarily, the prover will offer a computational concentrated numerical issue, and the verifier will request one of the numerous conceivable answers for the issue. On the off chance that the prover knows basic data identifying with the arrangement, it gives any of the asked for accessible arrangements on request. On the off chance that the prover does not know the basic data, it is computationally infeasible

for it to dependably give the asked for answer for the verifier. Normally, ZKP depend on some hard scientific issues, for example, the factorization of whole numbers or the discrete logarithm issue.

*D. Security Analysis of the Proposed Model*

- Case 1: At the point when the cloned node utilizes whatever other existing id with same unique finger impression.
- Case 2: At the point when the cloned node utilizes same id with same unique mark.
- Case 3: At the point when cloned node utilizes existing id with an alternate unique mark.
- Case 4: To efficiently identify clones with lowest communication cost
- Case 5: It manages network traffic evenly circulated over sensor nodes.

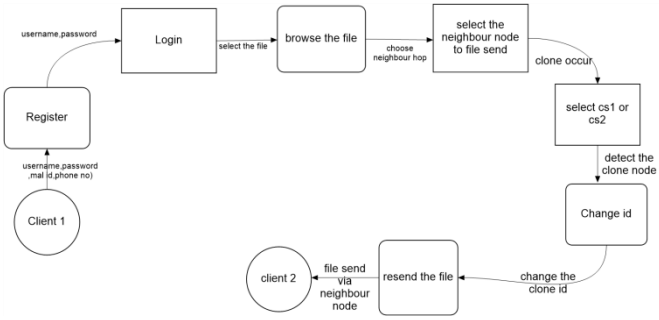



Fig. 1: Communication in Proposed Model

## III. PROPOSED CSI-1 & CSI-2 MODEL

CSI 1 algorithm used for constructing aggregation tree and detect the clone node. An aggregation tree needs to be constructed. A tree construction algorithm is TAG. In short, in TAG, the BS, as the root of tree, broadcasts a beacon message to the network. Each node, on the first receipt of the beacon message, rebroadcasts the beacon. Each node chooses the node from whom it receives the first beacon message as its parent node on the aggregation tree. After building the tree, each node knows which node acts as its parent node and which nodes are its children nodes. We assume that sensor nodes have been scheduled properly such that the data can be aggregated along the tree level by level. After construct the aggregation tree and then network owner wants to check whether there are clones in the network. Each node is supposed to receive a message from each of its children node, where is the aggregated measurement vector calculate set of children nodes on the aggregation tree, and is the set of aggregated measurement vectors calculated by the nodes in children. In CSI-1, leaf nodes actually do not need to send anything to their parent nodes. Each parent node of leaf node can generate the measurement vector of its children leaf nodes by first generating and then calculating. Note that the innocent nodes refuse to communicate with the nodes that do not take part in the tree construction. After receiving that, the node computes the aggregated measurement. After that no negative acknowledgement is sent from child node and forwards message. Here, the negative acknowledgement is defined as entire network is announcing the clone ID. CSI-2 algorithm used for detecting of clones with low communication. Each node computes and forwards the aggregated measurement vector in a similar way in CSI-1. Performing CS recovery on the aggregated measurement vector, the BS searches in the value column of lookup table for the match of the aggregated measurement value at the BS. When the value column of lookup table is sorted, the search can be accomplished efficiently by binary search. If a tuple vector, value is found, then vector would be the clone vector.

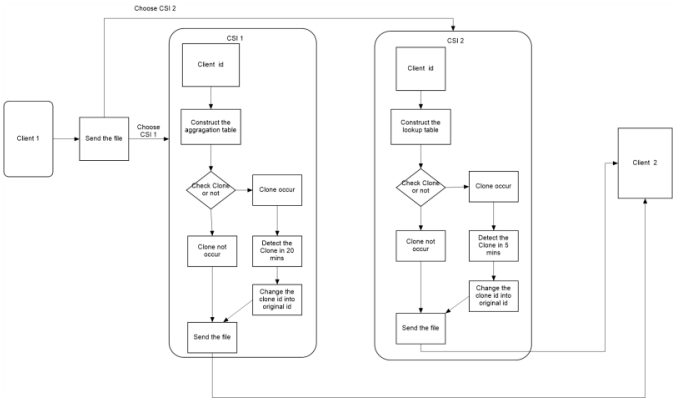



Fig. 2: Proposed CSI-1 & CSI-2 Model

## IV. EXPERIMENTAL SETUP

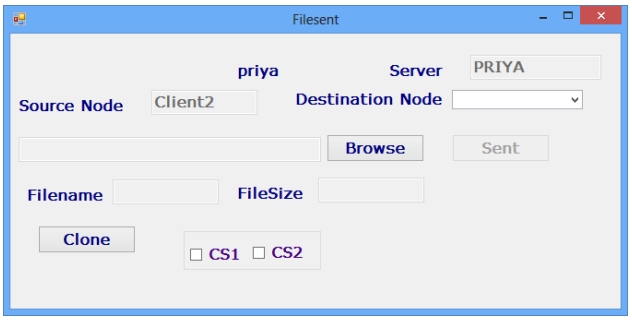
*1. Client registration:*
User enters the system with registration of required details. After getting the acknowledgement from system admin. Login access is enabled for user. Then upload the file to destination client.

*2. Witness finding strategy*
Witness finding strategy method is collecting all neighbor client information to source client. First send the request message from all client. All Client send the neighboring client information send to source client.

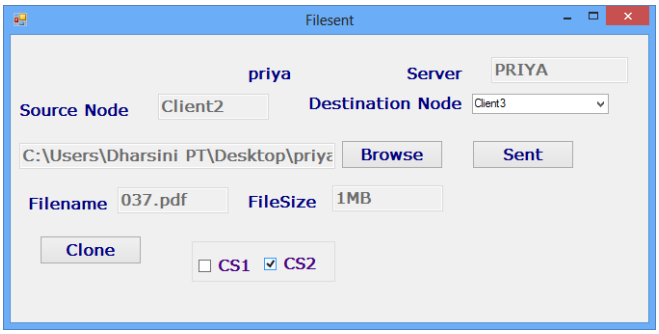
*3. Detect the clone using CSI 1*
Source client send the file through CSI 1 method. CSI 1 method first construct the aggregation tree. After, Check the cloning is occur or not. If cloning is occur. Detect the clone

in 20 mins. Then, change the clone id into original id. Finally, send the file to destination client.




*4. Detect the clone using CSI 2*Source client send the file through CSI 2 method. CSI 2 method first construct the lookup table. After, Check the cloning is occur or not. If cloning is occur. Detect the clone within 5 mins. Then, change the clone id into original id. Finally, send the file to destination client.




## V. CONCLUSION

In this manuscript, we proposed another security model to address three critical dynamic attacks to be specific cloning attack, MITM attack and Replay attack. We utilized the idea of zero knowledge protocol which guarantees non-transmission of urgent data between the prover and verifier. In our proposed, a novel clone detection framework, called CSI to overcome the previous clone detection problems. We introduced two algorithms are CSI-1 and CSI-2.The CSI-1 (Ordinary Compressed Sensing-Based Approach) algorithm used to constructed a aggregation tree and then detected clone. The CSI- 2 (Random Projection-Based Approach) is reduced the communication cost. Our proposed CSI method not only achieved lowest communication cost but also managed the network traffic evenly spread over sensor nodes. The presentation and security of CSI will be demonstrated feasibility of clone detection.

## REFERENCES

[1] T. Bonaci, P. Lee, L. Bushnell, and R. Poovendran, "*A convex optimization approach for clone detection in wireless sensor networks*," Pervasive Mobile Comput., vol. 9, no. 4, pp. 528–545, 2012.

[2] C. T. Chou, A. Ignjatovic, and W. Hu, *"Efficient computation of robust average of compressive sensing data in wireless sensor networks in the presence of sensor faults*," in Parallel Distrib. Syst., vol. 24, no. 8, pp. 1525–1534, Aug. 2013.

[3] K. Cho, M. Jo, T. Kwon, H.-H. Chen, and D. H. Lee, *"Classification and experimental analysis for clone detection approaches in wireless sensor networks*," in IEEE Syst. vol. 7, no. 1, pp. 26–35, Mar. 2013.

[4] M. Conti, R. Di Pietro, L. V. Mancini, and A. Mei, *"Distributed detection of clone attacks in wireless sensor networks,"* IEEE Trans. Dependable Secure Comput., vol. 8, no. 5, pp. 685–698, Sep./Oct. 2011.

[5] H. Chen, A. Perrig, and D. Song, *"Random key predistribution schemes for sensor networks,"* in Proc. IEEE Symp. Sec. Privacy, 2003, pp. 197– 213.

[6] E. J. Candès, J. K. Romberg, and T. Tao, *"Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information,"* IEEE Trans. Inf. Theory, vol. 52, no. 2, pp. 489–509, Feb. 2006.

[7] Compressive Sensing Resources [Online]. Available: http://dsp.rice.edu/ cs

[8] H. Choi, S. Zhu, and T. F. La Porta, *"SET: Detecting node clones in sensor networks,"* in Proc. Int. Conf. Sec. Privacy Commun. Netw. (Securecomm), 2007, pp. 341–350.

[9] Y.-C. Hu, A. Perrig, and D. Johnson, *"Packet leashes: A defense against wormhole attacks in wireless networks,"* in Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM), 2003, pp. 1976–1986.

[10] C.M.Yu, C.S.Lu, and S.Y.Kuo, *"CSI: Compressed sensing-based clone identification in sensor networks,"* in Proc. IEEE Int. Workshop Sensor Netw. Syst. Pervasive Comput. (PerSeNS), 2012, pp. 290–295.

[11] C.M.Yu, Y.T.Tsou, C.S Lu, and S.Y.Kuo, *"Localized algorithms for detection of node replication attacks in mobile sensor networks,"* IEEE Trans. Inf. Forensics Sec., vol. 8, no. 5, pp. 754–768, May 2013.

[12] B.Yu et al., *"Distributed data aggregation scheduling in wireless sensor networks,"* in Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM), 2009, pp. 2159–2167.

[13] B. Zhu, S. Setia, S. Jajodia, S. Roy, and L. Wang, *"Localized multicast: Efficient and distributed replica detection in large-scale sensor networks,"* IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 913–926, Jul. 2010.

[14] Y. Zeng et al., *"Random-walk based approach to detect clone attacks in wireless sensor networks,"* IEEE J. Sel. Areas Commun., vol 28, no. 5, pp. 677–691, Jun. 2010.

[15] M. Zhang, V.Khanapure, S.Chen, and X.Xiao, *"Memory efficient protocols for detecting node replication attacks in wireless sensor networks,"* in Proc. IEEE Int. Conf. Netw. Protocols (ICNP), 2009, pp. 284–293.