Exploratory Secure Transmission of Data with Semantic CPDA Rule in Wireless Sensor Networks

K.Bhagya Sri[1] A.Srinivasan[2]

[1.] M.Tech Scholar, Dept of Computer Science and Engineering, Sreenivasa Institute of Technology and Management Studies, Chittoor

[2.] Associate Professor, Dept of Computer Science and Engineering, Sreenivasa Institute of Technology and Management Studies, Chittoor.

Abstract: *-Data Aggregation in moderate hubs (called aggregator hubs) is a viable methodology for streamlining utilization of rare assets like data transfer capacity and vitality in Remote Sensor Networks (WSNs). Then again, in-system preparing represents an issue for the protection of the sensor information since individual information of sensor hubs should be known not aggregator hub before the collection procedure can be conveyed out. In utilizations of WSNs, protection protecting information collection has turn into a critical prerequisite due to delicate nature of the sensor information. This paper proposes a conventions and plans for this reason called CPDA - for completing added substance information collection in a protection saving way for application in WSNs. The plan has been very prevalent and surely understood. Regardless of the popularity of this convention, it has been found that the convention is powerless against assault and it is likewise not vitality productive. In this paper, we first present a brief best in class review on the present protection protecting information conglomeration conventions for WSNS. At that point we portray the CPDA convention and recognize its security weakness. At last, we exhibit how the convention can be made secure and vitality productive.*

Index Terms:-*wireless sensor network, privacy, data aggregation, cluster-based private data aggregation (CPDA); key distribution, collusion attack, malicious node*

I. INTRODUCTION

Lately, remote sensor systems (WSNs) havedrawn extensive consideration from the exploration group on issues going from hypothetical exploration to down to earth applications. Unique attributes of WSNs, suchas asset requirements on vitality and computational force and security have been all around characterized and generally examined. What has gotten less consideration, in any case, is the basic security concern on data being gathered, transmitted, and dissected in a WSN. Such private and touchy data may incorporate payload information gathered by sensors and transmitted through the system to a brought together information handling server. Case in point, a quiet's pulse, sugar level and other indispensable signs are typically of discriminating protection concern when observed by a restorative WSN which transmits the information to a remote healing center or specialist's office. Protection concerns might likewise emerge past information substance and may concentrate on connection data, for example, the area of a sensor starting information communication.

Effective countermeasure against the exposure of both information and setting focused private data is a crucial essential for sending of WSNs in certifiable applications. Security assurance has been broadly concentrated on in different fields identified with WSNs, for example, wired and remote systems administration, databases and information mining. In any case, the accompanying innate components of WSNs present remarkable difficulties for protection conservation in WSNs, and keep the current procedures from being straightforwardly transplanted:

(i) Uncontrollable environment: Sensors may must be conveyed to an environment wild by the protector, such asa front line, empowering a foe to dispatch physical assaults to catch sensor hubs or convey fake ones. As a result, a foe may recover private keys utilized for secure correspondence and decode any correspondence spied by the foe.

(ii) Sensor-hub asset requirements: battery-controlled sensor hubs for the most part have serious imperatives on their capacity to store, transform, and transmit the detected information. Therefore, the computational unpredictability and asset utilization of open key figures is normally considered inadmissible for WSNs.

(iii)Topological requirements: the constrained correspondence scope of sensor hubs in a WSN requires various bounces with a specific end goal to transmit information from the source to the base station. Such a multi-bounce plan requests distinctive hubs to take various movement loads. Specifically, a hub closer to the base station (i.e., information gathering and handling server) needs to hand-off information from hubs assist far from base station in expansion to transmitting its own produced information, prompting higher transmission rate. Such an unequal system activity example conveys

critical difficulties to the insurance of setting focused protection data. Particularly, if a foe holds the capacity of worldwide activity examination, watching the movement examples of distinctive hubs over the entire system, it can undoubtedly recognize the sink and trade off contextprivacy, or indeed, even control the sink hub to block the correct working of the WSN.

The exceptional difficulties for security protection in WSNs require the improvement of successful protection savingprocedures. Supporting proficient in-system information total while saving information security has risen as an essential prerequisite in various remote sensor system applications. As a key way to deal with satisfying this prerequisite of private information accumulation, disguised information aggregation(CDA) plans have been proposed in which numerous sourcenodes send encoded information to a sink along a merge casttree withaccumulation of figure content being performed over the route a bunch based private information aggregation(CPDA) conspire in which the sensor hubs are haphazardly conveyed into groups The clusterleaders are in charge of specifically conglomerating information from the bunch individuals, with the correspondence secured by a sharedkey between a couple of conveying hubs. The total capacity influences logarithmic properties of the polynomials to register the sought total esteem in a bunch. While the conglomeration is done at the aggregator hub in each group, it is ensured that no individual hub becomes more acquainted with the touchy private estimations of different hubs in the bunch.

The middle of the road total esteem in every bunch is further accumulated along the steering tree as the information bundles move to the sink hub. The protection objective of the plan is two-fold. To start with, the security of information must be ensured end-to-end. While just the sink could find out about the last accumulation result, every hub will have data of its own information and does not have any data about the information of different hubs.

Second, to diminish the correspondence overhead, the information from diverse source hubs must be productively joined by transitional hubs (i.e. accumulation) along the way. By the by, these halfway hubs ought not realize any data about the individual hubs' information. The creators ofthe CPDA plan have displayed execution results of the convention to exhibit the productivity and securityof the convention. The CPDA convention has turn out to be truly famous, and to the best of our insight, there has been no distinguished defenselessness of the convention distributed in the writing.

II. RELATED STUDY

Group based information transmission in WSNs, has been investigated via specialists keeping in mind the end goal to accomplish the system versatility what's more, administration, which augments hub lifetime and lessen data transmission utilization by utilizing neighborhood joint effort among sensor hubs. In a group based WSN (CWSN), each group has a pioneer sensor hub, viewed as bunch head (CH). A CH totals the information gathered by the leaf hubs (non-CH sensor hubs) in its group, and sends the collection to the base station (BS). The LEACH (Low-Energy Adaptive Grouping Hierarchy) convention displayed is a broadly known and powerful one to lessen and parity the aggregate vitality utilization for CWSNs. All together to counteract fast vitality utilization of the arrangement of CHs LEACH haphazardly pivots CHs among all sensor hubs in the system, in rounds.

Drain accomplishes upgrades in terms of system lifetime. Taking after the thought of LEACH, a number of conventions have been introduced, for example, APTEEN and PEACH which utilize comparable ideas of LEACH. Inthis paper, for comfort, we call this kind of bunch based conventions as LEACH-like conventions. Specialists have been generally considering CWSNs in the most recent decade in the writing. Nonetheless, the usage of the bunch based structural planning in this present reality is fairly entangled.

The plausibility of the key administration has been demonstrated in WSNs as of late, which repays the lack from applying the symmetric key administration for security Computerized mark is a standout amongst the most discriminating security offered by cryptography in key administration. frameworks, where the coupling between the general population key and the ID of the underwriter is acquired by means of a computerized testament . The Identity-Based advanced Signature (IBS) plan , in view of the trouble of considering whole numbers from Identity-Based Cryptography (IBC), is to infer a substance's open key from its personality data, e.g., from its name or ID number. As of late, the idea of IBS has been created as a key administration in WSNs for security. Carman first consolidated the advantages of IBS and key redistribution set into WSNs, and a few papers showed up as of late.

The IBOOS plan has been proposed keeping in mind the end goal to decrease the reckoning and stockpiling expenses of mark handling. A general system for developing online/logged off mark plans was presented The IBOOS plan could be successful for the key administration in WSNs. In particular, the disconnected from the net stage can be executed on a

sensor hub then again at the BS preceding correspondence, while the online stage is to be executed amid correspondence. Some IBOOS plans areintended for WSNs. The disconnected from the net mark in these plans, notwithstanding, is recomputed by an outsider and needs reusability, hence they are not suitable for CWS.

III. PROPOSED SCHEME

The Network Model

The fundamental thought of CPDA is to acquaint clamor with therawinformation detected from a WSN, such that an aggregator canobtain exact collected data yet not individual information focuses. This is like the information irritation approach broadly utilized as a part of protection saving information mining.However, dissimilar to in protection saving information mining where clamors are freely created (aimlessly) and along these lines prompts loose totaled results, the clamors in CPDA are deliberately intended to influence the collaboration between diverse sensor hubs, such that the exact accumulated qualities can be acquired by the aggregator. Specifically,

CPDA orders sensor hubs into two classifications: group pioneers and bunch individuals. There is an one-to-numerous mapping between the bunch pioneers and bunch individuals. The group pioneers are in charge of straightforwardly totaling information from group individuals, with the correspondence secured by an alternate shared key between any pair of imparting hubs.

The WSN is displayed as an associated diagram G(V, E), where Vrepresents the arrangement of senor hubs and Erepresents the arrangement of remote connections associating the sensor hubs. The quantity ofsensor hubs is taken as |V| = N. An information collection capacity is taken that totals the singular sensor readings. CPDA plan has focusedon added substance total capacity, singular sensor perusing at time moment to for hub i. For calculation of the total capacities, the accompanying necessities are to be fulfilled:

(i) Protection of the person sensor information is to be secured, i.e., every hubought to be known none other expect the hub itself,

(ii) The quantity of messages transmitted inside of the WSN for the purposeof information conglomeration ought to be kept at the very least, and

(iii) The conglomeration result ought to be as precise as could be expected under the circumstance

Key Distribution and Management

CPDA utilizes an irregular key conveyance system proposed in for encoding messages to avert message listening stealthily assaults. The key conveyance plan has three stages:

(i) Key predistribution,
(ii) Shared-key revelation, and
(iii) Way key foundation.

These stages are depicted quickly as takes after. An expansive key-pool of Z keys and their characters are first produced in the key predistribution stage. For every sensor hubs, z keys out of the aggregate Z keys are picked. These z keys structure a key ring for the sensor hub. Amid the key-revelation stage, every sensor hub recognizes which of its neighbors impart a typical key to itself byconjuring and trading revelation messages. In the event that a couple of neighbor hubs share a typical key, then it is conceivable to build up a protected connection between them.

In the way key foundation stage, an end-to-end way key is allocated to the sets of neighboring hubs who don't offer a typical key however can be associated by two or more multi-jump secure connections toward the end of the mutual keydiscovery stage. Toward the end of the key dispersion stage, the likelihood that any pair of hubs have no less than one normal key is given by (1):

$$Z_{\text{Connect}} = 1 - \frac{((Z-z)!)2}{(K-2k)!K!}$$

In the event that the likelihood that whatever other hub can overthe scrambled message by a given key is meant as z catch, then z overhearis given by (2):

$$Z_{\text{overhear}} = \frac{z1}{Z}$$

Attack Model

we exhibit a proficient assault on the CPDA total plan. The target of the assault is to demonstrate the powerlessness of the CPDA plan which can be suitably abused by a pernicious partaking sensor node.The expectation of the pernicious hub is to partake in the plan in such a path, to the point that it can become acquainted with the privatevalues (i.e., a, band c) of the taking an interest sensor hubs. For describingthe assault situation, we utilize the same illustration bunch comprising of three sensor hubs A, Band C. The hub Ais the group pioneer while Band Care the bunch individuals. We recognize two sorts of assaults: (i) assault by a vindictive clusterleader (e.g., hub An) and (ii) assault by a vindictive bunch part (e.g., either hub Borhub C). These two cases are depicted in detail in the accompanying sub-areas.

Modified CDPA for High Security and Robustness

In this segment, we talk about the adjustments needed on the existing CPDA plot so that a pernicious member hub can't dispatch the assault portrayed It might be noticed that, the fundamental weakness of the CPDA plan lies in the unhindered opportunity designated on the partaking hubs for creating their open seed qualities. no limitations on estimations of x, yand zrespectively while these qualities are

produced by the hubs. A vindictive aggressor abuses this flexibility to produce a discretionarily substantial open seed quality

To forestall such an assault, the CPDA convention should be adjusted. In this adjusted form, thenodes in a group make a scout the produced open seed values so that it is impractical for a vindictive participantto produce any subjectively vast seed worth. For a bunch with three hubs, such a requirement may be forced by the necessity thatthe total of any two open seeds must be more noteworthy than the thirdseed. In different words: x+ y> z, z+ x> y, and y+ z> x. In the event that these requirements are fulfilled by the created estimations of x, yand z, it will be inconceivable for any hub to dispatch the assault and get access to the private estimations of the other taking part hubs. In any case, regardless of the possibility that the above limitations on the estimations of x, y what's more, zare forced, the hubs ought to be watchful in picking the values for their mystery arbitrary number sets. In the event that twonodes happen to pick substantial qualities for their randomnumbers contrasted with those picked by the third hub, then itwill be workable for the third hub to become acquainted with the private estimations of the other two hubs. For instance, let us expect that hubs A furthermore, picked the estimations of r1 A, r2 A furthermore, r1 C, r2 C such that they are all much bigger than r1 B furthermore, r2 B - the private irregular number pair picked by hub B. It will be workable for hub Bto determine the estimations of aand c: the private estimations of hubs Aand Crespectively.

$$v_A^A / y^2 = a / y^2 + r_1^A / y + r_2^A = r_2^A$$
$$(v_B^A - r_2^A y^2) / y = a / y + r_1^A = r_1^A$$

In order to defend against the above vulnerability,the CPDA protocol needs further modification. In this modified version, after the values vAA, vAB, and vACare generated and shared by A, Band Crespectively, the nodes check whether the following constraints are satisfied: vAA+ vAB>vAC, vAB+ vAC>vAA, and vAC+ vAA>vAB. The nodes proceed for further execution of the algorithm only if the above three inequalities are satisfied. If all three inequalities are not satisfied, there will be a possibility that the random numbers generated by one node is much larger than those generated by other nodes – a scenario which indicates a possible attack by a malicious node

VI. CONCLUSION

In-network data aggregation in WSNs is a technique thatcombines partial results at the intermediate nodes en route to he base station (i.e. the node issuing the query),thereby reducing the communication overhead and optimizing the bandwidth utilization in the wireless links. However, this techniques raises privacy issues of the sensor nodes which needs to share their data with the aggregator node.In applications such as health care and military surveillance where the sensitivity of the private data of the sensors is very high, the aggregation has to be carried out in a privacy-preserving way, so that the sensitive data are not revealed to the aggregator. A very popular scheme for this purpose exists in the literature which is known as CPDA. Although, CPDA is in literature for quite some time now, no vulnerability of the protocol has been identified so far. In this paper, we have first shown a security vulnerability in the CPDA protocol, in which we have demonstrated how a malicious sensor node in a WSN can exploit the protocol in such a way that it gets access to the private sensitive values of its neighboring nodes while data aggregation process takes place in an aggregator. We have also proposed a suitable modification of the CPDA protocol to make it robust against this vulnerability and also to make it computationally more efficient. Future plan of workincludes experimental analysis to evaluate the performance of the proposed modified CPDA protocol and compare its computational and communication overhead with thoseof the existing privacy homomorphism-based encryption forsecuredata aggregation in WSNs.

V. REFERENCES

[1] T. Hara, V. I. Zadorozhny, and E. Buchmann, Wireless Sensor NetworkTechnologies for the Information Explosion Era, Stud. Comput.Intell.Springer-Verlag, 2010, vol. 278.

[2] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issuesin Wireless Sensor Networks," IEEE Commun. Surveys Tuts., vol. 8,no. 2, pp. 2–23, 2006.

[3] A. A. Abbasi and M. Younis, "A survey on clustering algorithms forwireless sensor networks," Comput. Commun., vol. 30, no. 14-15, pp.2826–2841, 2007.

[4] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "AnApplication-Specific Protocol Architecture for Wireless MicrosensorNetworks," IEEE Trans. Wireless Commun., vol. 1, no. 4, pp. 660–670,2002.

[5] A. Manjeshwar, Q.-A.Zeng, and D. P. Agrawal, "An Analytical Model
for Information Retrieval in Wireless Sensor Networks Using EnhancedbAPTEEN Protocol," IEEE Trans. Parallel Distrib. Syst., vol. 13, pp.1290–1302, 2002.

[6] S. Yi, J. Heo, Y. Cho et al., "PEACH: Power-efficient and adaptiveclustering hierarchy protocol for wireless sensor networks," Comput.Commun., vol. 30, no. 14-15, pp. 2842–2852, 2007.

[7] K. Pradeepa, W. R. Anne, and S. Duraisamy, "Design and Implementa-tion Issues of Clustering in Wireless Sensor Networks," Int. J. Comput.Applications, vol. 47, no. 11, pp. 23–28, 2012.

[8] L. B. Oliveira, A. Ferreira, M. A. Vilac¸a et al., "SecLEACH-On thesecurity of clustered sensor networks," Signal Process., vol. 87, pp.2882–2895, 2007.

[9] P. Banerjee, D. Jacobson, and S. Lahiri, "Security and performanceanalysis of a secure clustering protocol for sensor networks," in Proc.IEEE NCA, 2007, pp. 145–152.
[10] K. Zhang, C. Wang, and C. Wang, "A Secure Routing Protocol forCluster-Based Wireless Sensor Networks Using Group Key Manage-ment," in Proc. WiCOM, 2008, pp. 1–5.
[11] S. Sharma and S. K. Jena, "A Survey on Secure Hierarchical RoutingProtocols in Wireless Sensor Networks," in Proc. ICCCS, 2011, pp.146–151.
[12] G. Gaubatz, J. P. Kaps, E. Ozturk et al., "State of the Art in Ultra-Low Power Public Key Cryptography for Wireless Sensor Networks,"in Proc. IEEE PerCom Workshops, 2005, pp. 146–150.
[13] W. Diffie and M. Hellman, "New Directions in Cryptography," IEEETrans. Inf. Theory, vol. 22, no. 6, pp. 644–654, 1976.
[14] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," inLect. Notes.Comput. Sc. - CRYPTO, 1985, vol. 196, pp. 47–53.
[15] D. W. Carman, "New Directions in Sensor Network Key Management,"Int. J. Distrib. Sens. Netw., vol. 1, pp. 3–15, 2005.

AUTHOR PROFILE

K.Bhagya Sriis an M. Tech Scholar of Computer Science and Engineering at Sreenivasa Institute of Technology and Management studies, JNTU Anantapur, She Received B.Tech degree from SPMVV, Tirupati, India in 2013, and Her area of Interest are Secure Computing and Networking

A.Srinivasan is currently working as Associate Professor in SITAMS, Chittoor; His area of Interest is Grid Computing and Information Security