International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 8, August 2014)

Data Aggregation in Reverse Multicast Traffic for Sensor Networks

K. Apoorva
M. Tech Student
Dept. of CSE, MREC, Hyderabad, India
apoorva.kare@gmail.com

M. Swami Das
B.E(CSE), M. Tech(CSE), Ph. D
Associate Professor
Dept. of CSE, MREC, Hyderabad, India
msdas.520@gmail.com

Abstract: **For wireless device networks, knowledge aggregation schemes that cut back an oversized quantity of transmission is that the most sensible technique. In previous studies, homo-morphic encryptions are applied to hide communication throughout aggregation such enciphered knowledge is aggregate algebraically while not cryptography. Since aggregators collect knowledge while not cryptography, adversaries don't seem to be able to forge aggregate results by compromising them. However, these schemes don't seem to be satisfy multi-application environments. Second, these schemes become insecure just in case some device nodes square measure compromised. Third, these schemes don't give secure counting; so, they will suffer unauthorized aggregation attacks. Therefore, we have a tendency to propose a replacement hid knowledge aggregation theme extended from Boneh et al.'s homomorphic public encoding system. The planned theme has 3 contributions. First, it's designed for a multi application atmosphere. the bottom station extracts application-specific knowledge from aggregate ciphertexts. Next, it mitigates the impact of compromising attacks in single application environments. Finally, it degrades the harm from unauthorized aggregations. To prove the planned scheme's strength and potency, we have a tendency to conjointly conducted the great analyses and comparisons within the finish.**

Keywords: Aggregation, Homomorphic public Encryption, Symmetric Key, Database Asa Service, Attacker

1. INTRODUCTION

Wireless device Networks (WSNs), encompass thousands of device nodes (SN) that gather knowledge from deployed environments and it's utilized in lots of wealthy applications, like atmosphere observation, accident reportage, and military investigation. counting on the aim of every application, tin is tailor-made to scan completely different sorts of knowledge. The aggregators collect knowledge from a set of the network and combination the info and combination perform. Aggregation reduces the number of network traffic that helps to scale back energy consumption on device nodes in WSN, the aggregators in an exceedingly secure knowledge aggregation situation have to be compelled to rewrite the encrypted knowledge to perform aggregation. Girao et al [4] proposes AN additive and increasing homomorphic encoding that enables aggregation of encrypted knowledge and it's secure and economical. Concealed knowledge aggregation(CDA) schemes that square measure supported the homomorphic characteristics of a privacy homomorphism(PH) alter end-to-end encoding in wireless device networks. CDA needs that a key be distributed to a subgroup of nodes that kind a reverse-multicast routable region within the WSN. This key allows the nodes to perform end-to-end encoding wherever the corruption of 1 node, or a set of nodes. The CDA approach considerably reduces the energy consumption at individual nodes since no encoding and cryptography is performed. Hid knowledge Aggregation in Multiple Applications (CDAMA) is that the theme that has hid knowledge Aggregation (CDA) between multiple teams. CDAMA having 2 limitations once it combination multiple applications that shared in WSN will cut back the system value and improve system flexibility like

- CDA necessities give solutions to take care of knowledge privacy and cut back the communication overheads; corresponding cipher text should be aggregate.
- Aggregation of multi-application continues to be laborious although aggregation of cipher texts is feasible, as a result of the cryptography cannot extract application-specific aggregate result from a mixed cipher text.

A. Characteristics of CDAMA square measure as follows:

- Designed for multiple applications in WSN. during this characteristic, cipher text of various applications can't combination along.
- In CDAMA, cipher text of various applications combination into one cipher text.
- Designed for single application WSNs and it mitigates the impact of compromising tin through the development of multiple teams.
- Designed for secure enumeration. the bottom station doesn't knowledge several messages square measure aggregate from the decrypted aggregate result.

CDAMA having many problems together with economical implementation, cipher text length and curve choice. initial operations in CDAMA square measure supported scalar multiplication on elliptic curve points, skills that accelerate scalar multiplications which will enhance the performance of CDAMA. second the length of cipher texts isalso outlined thanks to deciding rock bottom sure of cipher text length for ample security.

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 8, August 2014)

B. CDAMA Requirements:

CDAMA needs information measure, security, knowledge integrity, authentication [4][8].

a)Bandwidth: The information measure overhead attributed to causation ciphertexts shouldn't need the transmission of huge amounts of further knowledge.
b)Provable Security: the protection level of the encoding theme ought to be measurable and it ought to be based mostly upon the ordinarily united hardness of a mathematical downside to be demonstrably computationally secure.
c)Data Integrity: Data integrity ensures the receiver that the received knowledge isn't altered in transit by AN soul. Integrity is enforced to confirm that info isn't altered in any sudden approach.
d)Authentication: it's necessary that the interface outlined between the user, the system and also the admin must give authentication. in an exceedingly device network, AN soul will inject the messages and also the authentication techniques will verify the identity of knowledge victimization isobilateral key. The privacy homomorphic encoding functions solely unidirectional authentication of device knowledge at the bottom station solely.
e) Authorization: Data authorization specifies access rights to resources and is powerfully associated with access management. Access management ought to stop unauthorized users from taking part in network resources.

C. *Varieties of Attacks:*

CDAMA faces many varieties of attacks[8], they're as follows;

a) Ciphertext Analysis:The most simple attack is that the analysis of encrypted packet; the soul needs to get info solely by deciphering cipher texts. In WSNs with a scarce domain of values, the attack will terribly expeditiously end in a deduction of the plaintexts.
b) KnownPlaintextAttack: The soul tries to work out secret info with the extra data of plaintexts.With known plaintext and corresponding cipher text, it's the aim of theadversary either to reveal the key key or a minimum of to collect further info which will be exploited to deduct malicious cipher texts or rewrite different messages.
c) physical property: Malleability is just variation of the attack that may generate the cipher text that's correct.
d) ForgePackets:An soul doesn't have to be compelled to modify existing knowledge, if she is ready to form properly encoded cipher text with a particular content. The assaulter may substitute the packets of perceived price that the forge done. A pH theme that's immune to maliciously cast packets should not enable any third party to form properly encoded messages a minimum of not while not having the ability to discover the interference throughout cryptography.

2. RELATED WORK

In WSN, sensor knowledge should be encrypted with one key to perform hid knowledge aggregation device nodes within the network should share a standard key and use it for encoding. employing a single isobilateral key within the network isn't secure as AN soul will pretend the aggregate results through compromising solely a device node.

Symmetric key based mostly privacy similarity is shown to be insecure for chosen plaintext attacks for a few specific parameter settingsas dropping or formation messages and sending false knowledge. Witness nodes {of knowledge|of knowledge|of information} aggregators alsoaggregate knowledge and cypher MACs to assist verify the correctness of the aggregators' data at base station as a result of the info validation is performed at base station, the transmission of false knowledge and MACs up to base station have an effect on adversely the employment of device network resources.

Due to their high process overhead, uneven key homomorphic encoding algorithms don't seem to be possible for device nodes. The privacy homomorphic encoding algorithmic program introduced by Domingo[3] Ferrer is isobilateral key based mostly. The hid knowledge aggregation algorithmic program that's planned that employs Domingo[3] Ferrer's privacy homomorphic encoding algorithmic program.

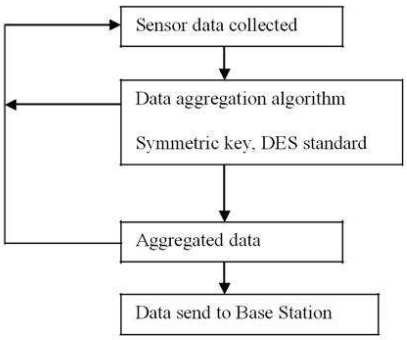

Fig 1. Architecture of Data aggregation algorithm

However so as to combination the info of the all network, the planned theme should uses a secret key known by all device nodes that ends up in give effective security to knowledge. If a device node is compromised, it will rewrite knowledge of any device node that is encrypted by the key key. Dolev Yao threat model [6], the assaulter will capture a device node and acquire all info hold on at intervals it. ought to the assaulter capture a set of device nodes, the likelihood that captured nodes square measure from identical region is above if the captured nodes square measure equally distributed over the WSN. Okamota and Uchiyama [9] planned a public-key cryptosystem with homomorphic properties, that is evidenced to be as secure. Castellucciaetal. [3] given AN economical aggregation of encrypted knowledge in wireless device networks that is additionally supported additively homomorphic options of the encoding theme supported AN extension of the sometime pad technique. This approach uses completely different keys per

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 8, August 2014)

device at the value of necessary sending the device ID list of the concerned observation nodes. Chan et al [7] gift the primary secure hierarchical knowledge aggregation theme supported aggregation commit verify, that forces the soul to arrange to its alternative of aggregation results so enable the sensors to verify whether or not their aggregation contribution is correct or not. Goldwasser and Micali [7] is to produce knowledge security, goal is to stop AN assaulter from gaining info regarding device knowledge.

3. PROPOSED WORK

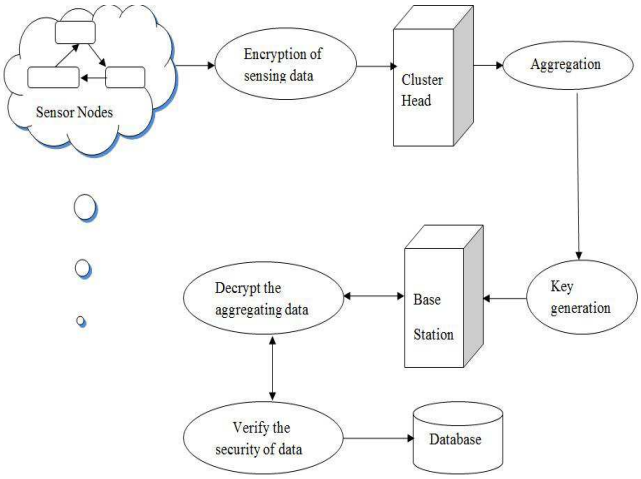

Fig 2. System Architecture

In WSN's, device nodes sends the encrypted knowledge that's capable of playacting some process the info to cluster head, CH organizes knowledge items received from tin into AN aggregate result, so forwards the result to the bottom station supported regular routing path. Aggregators would forward the results to subsequent hop when the aggregation done. so as to perform aggregation, aggregators square measure accustomed increase the period of time, tree-based or cluster networks force the intermediate nodes. Whenever the user wants info for the cluster or individual it'll send to the bachelor's degree. the bottom station received the request and split the cipher text. playacting the reverse aggregation the cipher text will rewrite to sends the info for users. The CH sends the result to aggregation, when aggregation done the results should be sends to base station. Base station currently will extract {the knowledge|the info|the information} (cipher text) with cryptography and verifies the decrypted data is secured and at last the info should be hold on in info repository.An important facet of encoding theme for aggregation in WSNs is that the sink node must bear in mind of the encryptors id's such it will regenerate the right key stream for cryptography functions. as a result of WSNs don't seem to be continuously reliable, it can not be expected that each one nodes reply to all or any requests. There want a mechanism for act the id's of the non-responding nodes to the bottom station.

4. IMPLEMENTATION

The process is split into many major tasks like device node and cluster aggregation, attacker, key generation, knowledge security.

Sensor Node and cluster Aggregation: Multi cluster knowledge will collect that is employed to form and separate the node and combination it. the combination node will analyse the cipher text, and may verify the message in cluster knowledge from multi cluster knowledge and produce the result that has to be hold on in base station.SN collect info from deployed environments and forward the data back to base station (BS) via multihop transmission supported a tree or a cluster topology. The tree-based or cluster networks force the intermediate nodes (a sub tree node or a cluster head) to perform aggregation, i.e., to be aggregators (AG). When aggregation done, AGs would forward the results to subsequent hop. The supply info for knowledge aggregators could originate from public knowledge. individual nodes summarize the knowledgesets so as to produce the next level read of obtainable data. When aggregation the cipher text is encoded when it's been {passed through|skilled|older|more matured|more experienced|more responsible|more established|seasoned|knowledgeable|versed|capable|competent| skillful|well-versed tried AND true|gone through|had|undergone|saw|felt|responded to|suffered} an encoding. The cipher text is that the product or combination of plain text and its encoding.

Attacker: Base station sends knowledge that is combination to make a cipher text, once encrypting a gaggle keys and a cipher key to provide a cipher text. Assaulter will collect the cipher text, then notice whether or not the info has assaulter, assaulter is within the text then analyse the text challenge to user if the assaulter isn't gift in cipher text then rewrite the info and send to user. soul needs to send the solid messages to cheat the bachelor's degree although she doesn't apprehend the key key. assaulter could be a special form of player, typically one whose role involves aggressive knowledge. a gaggle secret is a cryptologic key that's shared between teams of users. cluster key square measure distance by causation them to individual users physically or cipher severally for every user victimization either that user's pre distributed non-public key. Secure aggregation is needed once AN assaulter could capture secret knowledge as device networks square measure vulnerable. isobilateral key cryptography algorithms square measure attainable to achieving the secured knowledge.

Key Generation: Cluster Head will combination {the knowledge|the info|the information} sent by a device when aggregation the Cluster Head will generate a key superimposed to the aggregate data, when aggregation finally the info square measure sent to base station. Key generation is that the method of generating keys for cryptosystem. A secret is accustomed cipher or rewrite no matter knowledge is being encrypted or decrypted. Key Generator objects square measure

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 8, August 2014)

reusable, i.e., when a key has been generated, identical Key Generator object is re-used to come up with additional keys. There square measure 2 ways in which to come up with a key: in AN algorithm-independent manner, AND in an algorithm-specific manner. The sole distinction between the 2 is that the low-level formatting of the thing.

Data Security: Initially the bottom station will verifies the key from the aggregate knowledge sent by the Cluster Head, when validatory the keys the bottom station will rewrite the aggregate knowledge. Knowledge security is employed to protective a info from damaging forces or unwanted actions of unauthorized users.

5. CONCLUSION

For a multi-application atmosphere, CDAMA is that the initial hid knowledge aggregation theme. Through CDAMA, the ciphertexts from distinct applications is aggregate, however not mixed. For one application atmosphere, CDAMA continues to be safer than different hid knowledge aggregation schemes. once compromising attacks occur in WSNs, CDAMA mitigates the impact and reduces the harm to a suitable condition. Besides higher than applications, CDAMA is that the initial hid knowledge aggregation theme that supports secure enumeration. the bottom station would apprehend the precise range of messages aggregate, creating selective or perennial aggregation attacks impracticable. Finally, the performance analysis shows that CDAMA is applicable on WSNs whereas the amount of teams or applications isn't massive.

REFERENCES

[1]. Liu and P. Ning, (2008) "TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks," Proc. Int'l Conf. Information Processing in Sensor Networks (IPSN'08), pp.245-256.
[2]. Castelluccia, E. Mykletun, and G. Tsudik, (2005) "Efficient Aggregation of Encrypted Data in Wireless Sensor Networks,"Proc.Second Ann. Int'l Conf. Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous'05), pp.109-117.
[3]. Westhoff, J. Girao, and M. Acharya, (2006) "Concealed Data Aggregation for Reverse Multicast Traffic in Sensor Networks: Encryption, Key Distribution, and Routing Adaptation," IEEE Trans. Mobile Computing, vol.5, no. 10, pp. 1417-1431.
[4]. Mykletun, J. Girao, and D. Westhoff, (2006) "Public Key Based Cryptoschemes for Data Concealment in Wireless Sensor Networks," Proc. IEEE Int'l Conf. Comm. (ICC'06), vol.5.
[5]. H. Sanli, S. Ozdemir, and H. Cam, (2004) "SRDA: Secure Reference-based Data Aggregation Protocol for Wireless Sensor Networks," Proc. IEEE 60th Vehicular Technology Conf. (VTC'04-Fall), vol.7.
[6]. L. Oliveira, D. Aranha, E. Morais, F. Daguano, J. Lopez, and R. Dahab, (2007) "TinyTate: Computing the Tate Pairing in Resource-Constrained Sensor Nodes," Proc. IEEE Sixth Int'l Symp. Network Computing and Applications (NCA'07), pp.318-323.
[7]. R. Min and A. Chandrakasan, (2001) "Energy-Efficient Communication for Ad-Hoc Wireless Sensor Networks," Proc. Conf.
[8]. Record of the 35thAsilomar Conf. Signals, Systems and Computers, vol.1.
[9]. S. Peter, D. Westhoff, and C. Castelluccia, (2010) "A Survey on the Encryption of Convergecast-Traffic with In-Network Processing," IEEE Trans. Dependable and Secure Computing, vol.7, no.1, pp.20-34.
[10]. S. Zhu, S. Setia, and S. Jajodia, (2006) "LEAP+: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," ACM Trans. Sensor Networks, vol.2, no.4, pp. 500-528.
[11]. Y. Wu, D. Ma, T. Li, and R. H. Deng, (2004) "Classify Encrypted Data in Wireless Sensor Networks," Proc. IEEE 60th Vehicular Technology Conf., pp.3236-3239.