ISSN (Online): 2455-7838
SJIF Impact Factor (2017): 5.705

EPRA International Journal of

Research & Development

(IJRD)

Monthly Peer Reviewed & Indexed International Online Journal

Volume: 3, Issue:11,November 2018

Published By :
EPRA Journals

SJIF Impact Factor: 5.705 Volume: 3 | Issue: 11 | November | 2018 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)

A SURVEY OF ID BASED DATA AGGREGATION WIRELESS SENSOR NETWORK

S.Maraimathi
Computer instructor, Coimbatore

D.Umanandhini
Assistant Professor, Department of Computer Science, Kovai Kalaimagal Collage of Arts and Science Coimbatore, Tamil Nadu, India

ABSTRACT
Data Aggregation is an important topic and an appropriate strategy in decreasing the vitality utilization of sensors nodes in Wireless sensor network (WSN's) for managing secure and productive big data aggregation. The wireless sensor networks have been comprehensively connected, for example, target following and condition remote monitoring. However, data can be easily compromised by a vast of attacks, such as data interception and tampering of data. Data integrity protection is proposed, gives an identity-based aggregate signature scheme for wireless sensor networks with a designated verifier. The aggregate signature scheme keeps data integrity, can reduce bandwidth and storage cost. Furthermore, the security of the scheme is effectively presented based on the computation of Diffie-Hellman random oracle model.
KEYWORDS: *Data Aggregation, storage cost, bandwidth, temperature, sound, pressure*

1. INTRODUCTION

Wireless device networks (WSN), generally referred to as wireless device and mechanism networks (WSAN) square measure spatially distributed autonomous sensors to observe physical or environmental conditions, like temperature, sound, pressure, etc. and to hand and glove pass their information through the network to a main location. The lot of fashionable networks square measure bi-directional, conjointly sanctionative management of device activity. The event of wireless device networks was impelled by military applications like parcel surveillance; nowadays such networks square measure utilized in several industrial and shopper applications, like process watching and management, machine health watching, and so on.

In device network important facet is that the flow of knowledge. It contains info which can be vital for a few applications. Thus there ought to be a secure information transmission. However maintaining security is troublesome for device nodes as a result of they need restricted energy and restricted memory capability. Reports square measure made up of the information received from device nodes. These report should be demonstrate and reach while not modification to the bottom station.WSN square measure utilized in several application like military, ecological and health connected space. This application is also encircled by harsh, neglected and sometimes adversarial physical surroundings. Thus secure and economical information transmission (SET) is important and is vital issue in WSN.

In huge information era, digital universe grows in beautiful speed that is made by rising new services, like social network, cloud computing and net of things. huge information square measure gathered by present

wireless device networks, aerial sensory technologies, software system logs, information-sensing mobile devices, microphones, cameras, etc. and therefore the wireless device network is one in all the extremely anticipated key contributors of the massive information within the future networks. Wireless device networks (WSNs), with an oversized variety of low cost, tiny and extremely unnatural device nodes sense the physical world, has terribly broad application prospects each in military and civilian usage, as well as military target following and police work, animal habitats watching, medicine health watching, important facilities following. It will be utilized in some hazard environments, like in nuclear energy plants. Because of the exceptional blessings, comprehensive attention has been dedicated to WSNs, and variety of schemes is bestowed.

2. RELATED WORK

In 1984, Shamir introduced the identity-based (ID-based) cryptography that eases the key management drawback by eliminating public key certificates. In AN ID-based cryptography, the user's public secret is simply generated from this user's any distinctive identity info (e.g. the serial variety, a movable variety, AN email address, etc), that is assumed to be publically renowned. A trustworthy third party, referred to as the non-public key generator (PKG), generates and problems on the QT the corresponding non-public keys for all users employing a master secret key. Therefore, in AN ID-based signature (IBS) system, verification algorithmic rule solely involves the signature try, some public parameters and therefore the identity info of signer, while not exploitation an extra certificate [1].

In 2003, Boneh et al. introduced A mixture signature theme, which may compress multiple signatures generated by totally different completely users on different messages into one short mixture signature. The combination signature's validity will be reminiscent of the validity of each signature that is employed to come up with the combination signature. That's to mention, the combination signature is validity if and providing every individual signer extremely signed its original message, severally. Hence, aggregation is beneficial technique in reducing storage value and information measure, and may be a decisive building block in some settings, like information aggregation for WSNs, securing border entrance protocols and huge scale electronic legal system, etc. during this paper, combining the highlights of mixture signature theme and ID-based cryptography, we tend to provide AN ID-based mixture signature (IBAS) theme for WSNs in cluster-based technique [2].

3. METHODOLOGY

From our survey of existing secure knowledge Aggregation Techniques we have a tendency to acknowledge that the present approaches projected for secure knowledge aggregation don't provide the desired safety features viz. confidentiality, integrity and authentication along. Therefore, with the motivation to boost upon an equivalent, we have a tendency to propose a brand new approach that gives ALL of those attributes. Our approach relies on public key cryptography, victimization homomorphic encoding and additive digital signatures to realize confidentiality, message integrity and authentication for knowledge aggregation in wireless detector networks.

3.1 Totally different Wireless recharging techniques

Totally different Wireless recharging techniques just in case of powerfully coupled resonance one mobile charger travels within the setting to recharge energy to the sensing element nodes, principally resonance can work only the space is a smaller amount between the sensing element node and reversible resonance.

Battery free programmable RFID sensing element device in Wireless identification and sensing platform (WISP).WISP functions in biface line and its wireless power comes within the vary of few meters. However potency is a smaller amount and freedom is a lot of RFID-based wireless reversible sensing element network to attenuate the communication delay supported moving flight. The downside is RFID Technology consumes a lot of energy and packet transmission is slow.

3.2 Single Mobile Chargers Protocol

This algorithm recharges sensing element nodes in additional economical manner compared with alternative approaches. To extend the network lifespan, by mobile automaton carrying the charger with enough energy. This technique can properly once it distinctive the bottleneck nodes to recharge. It has been known wireless reversible sensing element network has the charging delay. Best conceivable development procedure of the charger, time to charge all nodes put in vitality storage over a foothold are decreased. Drawback featured here RFID reader's area unit terribly expensive. It has been planned Qi-Ferry(QiF) that physically holds energy and travels a WSN to wirelessly charge sensing element batteries therefore as increase the network lifespan. Downside of this Qi-Ferry is within which direction QiF ought to move and the way several nodes it charges.

3.3. Multiple Mobile Chargers Protocol

It has known usage of multiple mobile chargers is new manner recharging to extend the lifespan of the network. Main exchange is however Mobile charger coordinates with one another and within which directions mobile charger ought to study the multiple mobile chargers give a lot of measurability and strength compared with single mobile charger.

Communication protocol used here is known as information Networking (NDN).Tradeoff here is emergency charging. Reducing the quantity mobile charger within the 2nd network. Forward uniform consumption of energy all told nodes, forward sensing element nodes have constant energy depletion rate. Distance Constraint Vehicle Routing by reduction. Downside is once there's a non –uniform consumption of energy.

3.4. Coincidental Wireless Charging

It has been found that wireless charging vehicle charges multiple sensing element nodes at the same time. Advantage is it reduces variety of power sources needed within the network. Disadvantage is for extended distance poses a lot of loss of the energy. It have investigated that energy is transferred to sensing element nodes wirelessly within the economical manner by wireless charging vehicle. So as to extend the network lifespan, performance of charging can degrade once for extended distance between charger and node. It explore however measurability drawback happens in multi-node charging technology during a WSN. Attributable to that region Wireless charging vehicle (WCV) take a visit within the network during a timely fashion and charges the sensing element nodes. On each trip WCV takes vacation then goes for next trip. They need used discretization and a completely unique Reformulation-Linearization Technique (RLT) to found the close to optimum resolution. However reformulating the non linear drawback to linear one, the process quality could be a major drawback.

3.5. Cooperative Mobile Charging

Thought-about Quality of observance (QoM) drawback in WRSN. Provides economical charging distribution model to sensing element nodes, programming is principally featured here. Mobile charger will act as energy transfer to sensing element nodes furthermore as an information collector to order increase network lifespan.

4. SECURITY WANTS IN INFORMATION AGGREGATION

Information Aggregation in wireless sensing element network is a vital technique in addition as security to mass information is a vital issue. In some vital application like military police investigation and numerous life vital application information transmission, information aggregation, and information reception ought to be during a secured and energy economical approach. Thus to attain this several facts ought to be thought of such as: Confidentiality of information, Integrity of information, and Freshness of information, supply Authentication, and Secure Node localization [5].

1) Confidentiality of Data: It assures that associate degree unauthorized user couldn't access the non-public or counseling and information ought to be prevented from passive attack. By exploitation secret key information may be encrypted and sent to the receiver node. Each routing info and detected information ought to be maintained in secure approach.

2) Integrity of Data: Integrity of information assures that the information on the network area unit modified solely by approved user not any compromised nodes. It implies that, there's no modification, rearrangement within the received information. It ensures that information that needs to send shouldn't be corrupted before reaching the destination. This can be vital issue as a result of compromised node can amendment the information by inserting false information to the mass data.

3) Freshness of information: Data freshness is critical to stop the reply of previous messages at human node. Performance of network and energy may be effectively employed by achieving information freshness.

4) Secure Node localization: Node localization is incredibly vital issue in WSN thus it ought to be unbroken secure and will not be accessed by malicious node. If location of sensing element node is unconcealed to malicious node then all routing info conjointly unconcealed thus node location ought to be secure.

5) Supply Authentication: information Authentication ensures that received information ought to be identical as original information. Supply authentication permits that the information is distributed solely by the particular sender. Supply authentication will forestall the info from Sybil attack within which associate degree wrongdoer gain access to any node and capture the keep information.

Attacks on WSN Aggregation: On wireless sensing element network numerous quite attacks area unit potential as a result of it deployed within the surroundings that isn't secure and have less physical security to the sensing element nodes. On totally {different completely different} schemes different kind of attacks area unit performed by the somebody to interrupt the safety.

There's temporary discussion of those attacks given below:

1) Node Compromise attack: During this kind of attack the wrongdoer gain management over the deployed sensing element node and takes info keep on the sensing element nodes. Compromised node will insert the false information bit within the already keep true information. If associate degree somebody gains access to the human node then information isn't secured within the network.

2) Sybil Attack: During this attack wrongdoer will build multiple identities and affects numerous information aggregation techniques in many ways. When making multiple faux ids, it participates in

election of human nodes and tries to elect the malicious node as human node. Then it affects the information at the human node.

3) Denial of Service attack: During this kind of attack, wrongdoer jams the signal through interfere the radio frequencies by sending radio signals on the network. During this attack the human node refuses to combination {the information the info the information} gathered from numerous sensing element nodes and helps data from routing in higher levels.

4) Selective Forwarding Attack: Unremarkably sensing element nodes forward the information that it receives from alternative sensing element nodes. However during this attack the compromise node doesn't do this and have an effect on the information at human node. Any compromised node will launch the selective forwarding attack.

5) Replay Attack: During this from the network wrongdoer takes management on the traffic and record the traffic. Then mislead the human node by replays the recorded traffic and affects the result that is mass from the human node.

6) Injection Attack: During this the wrongdoer injects the incorrect information into the network. Within the method of aggregation this wrong information can lead to false mass information.

5. CONCLUSION

We introduce a novel coalition attack scenario against number of existing PPT algorithms. Moreover, we propose an improvement for ID-Based Aggregate Signature Scheme by providing an initial approximation of trustworthiness of sensor nodes which makes the data not only coalition free, but also more secure and efficient. We make use of Elliptic Curve Cryptography (ECC) and Diffie-Hellman Assumption for the process. In future works we will investigate whether our approach can protect against compromised aggregators to provide privacy over the data transmitted. We also planned to improvement our approach in deployed sensor network.

6. REFERENCE

1. *A. Shamir, "Identity-based cryptosystems and signature schemes," in Proc .CRYPTO 1984, Santa Barbara, California, USA, August 19-22, Springer-Verlag, Berlin LNCS, vol. 196, pp. 47-53, 1984.*
2. *D. Boneh, C. Gentry, B. Lynn and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps", in Proc. Eurocrypt 2003, Warsaw, Poland. LNCS, pp. 416-432, 2003.*
3. *X. Liu, R. Choo, R. Deng, R. Lu, "Efficient and privacy-preserving outsourced calculation of rational numbers," IEEE Transactions on Dependable and Secure Computing, 2016, doi: 10.1109/TDSC.2016.2536601.*
4. *H. Li, X. Lin, H. Yang, X. Liang, R. Lu, and X. Shen, "EPPDR: An Efficient Privacy-Preserving Demand Response Scheme with Adaptive Key Evolution in Smart Grid," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no.8, pp. 2053-2064, 2014.*
5. *I.F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A survey on sensor networks," IEEE Commun. Mag., vol. 40, no. 8, pp. 102-114, 2002.*
6. *G. Gentry and Z. Ramzan, "Identity-based aggregate signatures," in Proc. Public Key Cryptography, LNCS vol. 3958, pp. 257-273, 2006.*
7. *Z. Fu, X. Sun, Q. Liu, L. Zhou, J. Shu, "Achieving Efficient Cloud Search Services: Multi-keyword Ranked Search over Encrypted Cloud Data Supporting Parallel Computing," IEICE Transactions on Communications, vol. E98-B, no. 1, pp.190-200, 2015.*
8. *I. Hashem, I. Yaqoob, N. Anuar, et al., "The rise of "big data" on cloud computing: Review and open research issues," Information Systems, vol. 47, no. 47, pp. 98-115, 2015.*
9. *H. Li, Y. Yang, T. Luan, X. Liang, L. Zhou and X. Shen, "Enabling Fine-grained Multi-keyword Search Supporting Classified Sub-dictionaries over Encrypted Cloud Data," IEEE Transactions on Dependable and Secure Computing, DOI10.1109/TDSC.2015.2406704, 2015.*
10. *H. Li, D. Liu, Y. Dai and T. Luan, "Engineering Searchable Encryption of Mobile Cloud Networks: When QoE Meets QoP," IEEE Wireless Communications, vol. 22, no. 4, pp. 74-80, 2015.*