Secure grouping data transmission scheme for Multiple Applications in Wireless Sensor Network

A.ASHOK [a], M.CHINNADURAI [b],
[a] Department Of CSE, E.G.S.Pillai Engineering College, Tamilnadu, India.
[b] Assistant Professer, Department Of IT, E.G.S.Pillai Engineering College, Tamilnadu, India.

ABSTRACT:

Data aggregation system is the majority sensible technique for wireless sensor networks. It reduces a large amount of communication. To screen announcement during aggregation homomorphism encryptions have been practical in previous be taught. So the enciphered data can be aggregated algebraically without decryption. Although data aggregation could considerably reduce broadcast, it is defenseless to some attacks. However, these schemes failed to satisfy multi-application surroundings. The main drawback of this scheme is that, it become insecure in case a number of sensor nodes are compromised. Also, these schemes do not provide secure counting. Thus, it is suffer due to unauthorized aggregation attacks. An alternative move toward for this problem is to collective encrypted messages in a straight line from SN, thereby avoid the forgery of aggregate result. To end these drawbacks, we propose a new hidden data aggregation system called CDAMA, provide CDA connecting multiple groups. It is extensive from homomorphism community encryption system. There are three contributions in the proposed system. First, it is intended a multi-application surroundings. Next, it mitigates the crash of compromising attack in single request environments. Compared with conservative schemes, CDAMA mitigates the collision of compromise SN from beginning to end the construction of manifold groups. It reduces the damage from illegal aggregations.

Keywords: CDAMA, WSN, SN, CDA, BS, AG

I. INTRODUCTION

The expansion of wireless sensor networks was aggravated by military application such as battlefield observation; today such networks are used in numerous industrial and customer applications, such as manufacturing process monitoring and manage, machine health monitoring, and so on. Each such sensor system node has characteristically several parts: a radio transceiver with an interior antenna or association to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an power source, more often than not a battery or an embedded form of authority harvesting.

Wireless communication is the transport of information flanked by two or more points that are not associated by an electrical conductor. The most ordinary wireless technology use radio. With radio influence distances can be short, such as a few meters for television or as far as thousands or even millions of kilometers for deep-space radio communications. It encompasses various types of fixed, mobile, and portable applications, including two-way radios, cellular telephones, personal digital assistants (PDAs), and wireless networking.

Other examples of applications of radio wireless technology include GPS units, garage door openers, wireless computer mice, keyboards and headsets, headphones, radio receivers, satellite television, broadcast television and cordless telephones. Somewhat less common methods of achieving wireless infrastructure include the use of other electromagnetic wireless technology, such as light, attractive, or electric fields or the use of sound. Wireless networking is used to meet a lot of needs. Perhaps the most ordinary use is to connect laptop user who travel from site to position.

Another ordinary use is for movable networks that connect via settlement. A wireless transmission technique is a logical option to network a LAN section that must frequently alter locations. The following situation justify the use of wireless knowledge: To span a coldness beyond the capability of typical wiring, To provide a endorsement infrastructure link in case of normal system failure, To link moveable or temporary workstations, To conquer situations where normal cabling is difficult or financially not practical, or To remotely connect mobile users or networks.

A wireless sensor network (WSN) consists of spatially distributed independent sensors to monitor physical or ecological conditions, such as hotness, sound, pressure, and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. There is also no centralized body to allocate the resources and they have to be self-organized. The data gathered from wireless sensor networks is more often than not saved in the form of arithmetical data in a central base station. Additionally, the Open Geospatial Consortium (OGC) is specify standards for interoperability interfaces and metadata encodings that enable genuine time integration of varied sensor webs into the Internet, allow any individual to monitor or manage Wireless Sensor Networks from side to side a Web Browser. As nodes can examine the data they forward they know how to measure averages or directionality for example of reading from other nodes. This kind of data being without a job due to the spatial association between sensor comments inspires the technique for in-network data aggregation and mining.

II. RELATED WORK

Typically sensors are used for such a consequences have focused on the categorization based on signals obtain at a single or few sensors and process in a centralized way. Hence this existing fallout is only partially helpful for a WDSN request. It's considering the completion of such a task in a WDSN environment. Each sensor in the WDSN will be prepared with a microphone or a geophone. Upon discovery of the presence of a means of shipping in the neighborhood of the sensor, the on-board processor will extract attribute vectors based on the acoustic or seismic signal sense by the sensors. In a wireless sensor network, the communication bandwidth is very limited. Hence, instead of sending the characteristic vector, a local prototype classifier at each sensor node will first make a local decision on what type of the vehicle is based on its own trait vector. Statistically, this is a manifold hypotheses testing difficulty. The probability of correct categorization can also be estimated. The local choice, together with the estimated likelihood of being a correct decision after that can be encoded and transmit efficiently via the wireless strait to a local fusion center prepared for decision synthesis.

Sensor webs consisting of nodes by way of partial battery power and wireless connections are deployed to collect useful in sequence from the field. Gathering sensed in sequence in an energy efficient approach is critical to in commission the sensor network for a long period of time. A data collection problem is defined where, in a round of communication, each sensor node has a packet to be sent to the distant base station. There is some fixed amount of energy cost in the electronics when transmitting or receiving a packet and a variable cost when transmitting a packet which depends on the distance of transmission. If each node transmits its sensed data directly to the base station, then it will deplete its power quickly. The LEACH protocol presented elegant solution where clusters are formed to fuse data before transmitting to the base station. By randomizing the cluster-heads chosen to transmit to the base station, LEACH achieves a factor of 8 improvement compared to direct transmissions, as measured in terms of when nodes die. An improved version of LEACH, called LEACH-C, is presented, where the central base station performs the clustering to improve energy efficiency.

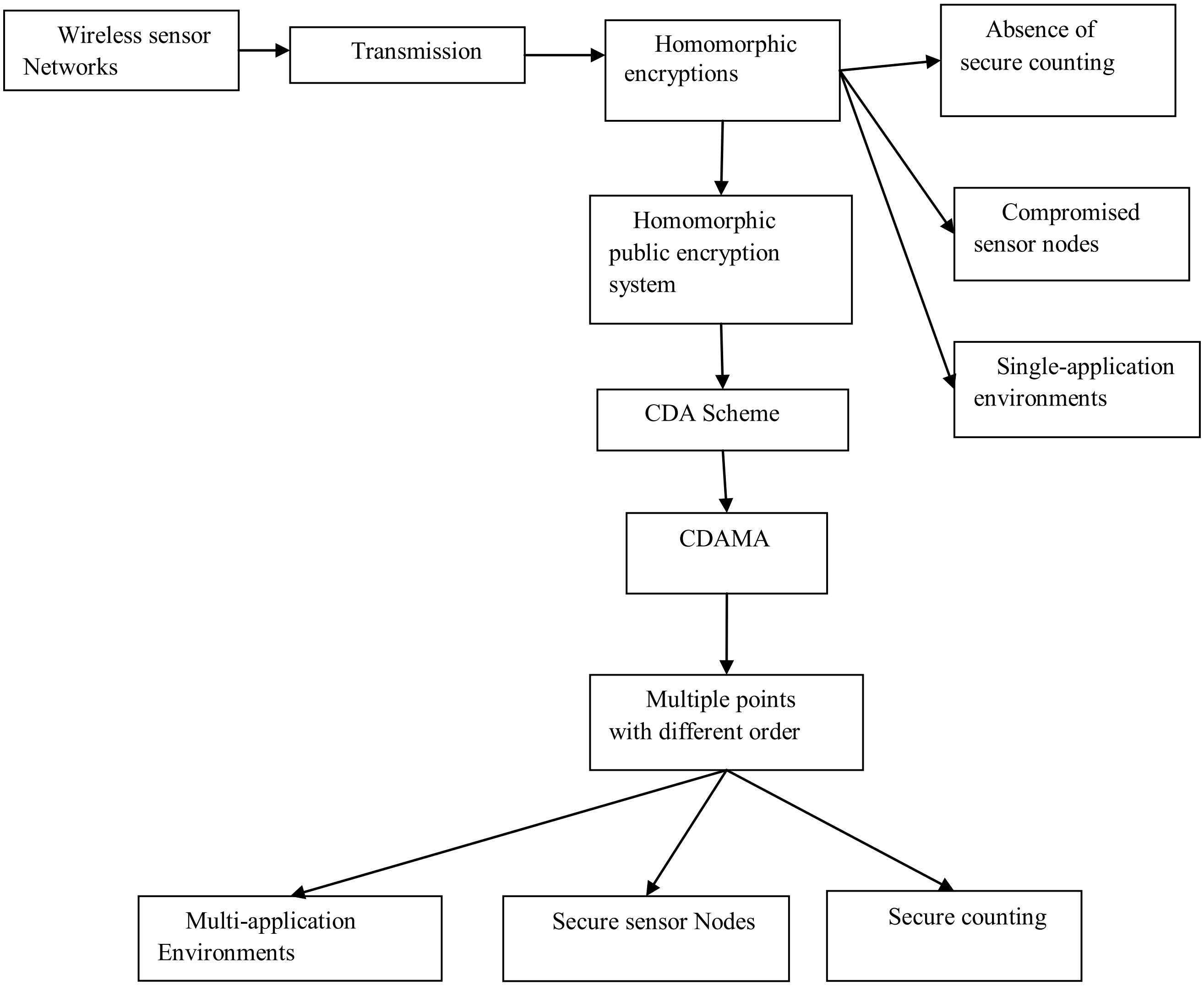
Wireless sensor networks (WSNs) constitute an emerging technology that has recently received significant attention both from industry and academia. They have an ever-widening range of attractive applications, such as in disaster and environmental monitoring, wildlife habitat monitoring, health monitoring, target tracking, intrusion detection, and battlefield surveillance. A WSN consists of a large number of sensor nodes equipped with limited and irreplaceable batteries which make energy efficiency a major concern. Data aggregation is a promised technique aiming to conserve energy by reducing the number of packet trans- missions through the network where communication costs (transmission power) are usually more expensive than computing costs. The two necessary conditions for an efficient data aggregation are spatial and temporal convergence. Indeed, the main challenges are to build up proper routes and also apply efficient scheduling mechanisms to the packets in such a way that they have more chance to meet at the same node at the same time. Actually, different streams are aggregated if they happen to intersect on their way to the sink. Approaching this goal, we have to hold packets in intermediate nodes to promote aggregation efficiency. More waiting time can lead to the collection of more data, the increase of aggregation gain, and vice versa. Therefore, data aggregation has a tradeoff relationship with delay. Finally, aggregation is a key yet time-consuming functionality in WSNs. Although energy efficiency is usually the primary concern in WSNs, the requirement of real-time communication is becoming more and more important in emerging applications.

III. PROPOSED SYSTEM

The proposed scheme, called CDAMA, provide CDA flanked by manifold groups. Essentially, CDAMA is an alteration CH scheme. SN collect in order from deployed environment and its onward the in sequence back to base station (BS) by means of multi hop broadcast based on a hierarchy or a cluster topology. The accumulate transmission carry large liveliness cost for midway nodes. To increase the existence, tree-based or cluster networks force the transitional nodes (a sub tree node or a cluster head) to carry out aggregation (AG). After aggregation done, AGs would forward the consequences to the next hop. In general, the information is able to be aggregated via arithmetical operations. Here, we also presume three sensible request scenarios for CDAMA, all of which can be realized through only CDAMA. The first situation is intended for multi-application WSNs. In practice, SN having dissimilar purposes, e.g., smoke sound the fear and thermometer sensors may be deployed in the same surroundings. If we apply conservative concealed data aggregation scheme the cipher texts of poles apart applications cannot be aggregated together; or else, the decrypted aggregated outcome will be incorrect.

The no more than solution is to collective the cipher texts of dissimilar application separately. As a result, the broadcast cost grows as the numeral of the application increase. By CDAMA, the cipher texts from dissimilar applications can be encapsulated into “only” one cipher text. Conversely, the base position can extract application-specific plaintexts via the matching secret keys. The second situation is designed for solitary application WSNs. compare with conservative schemes; CDAMA mitigate the impact of compromise SN through the building of multiple groups. An adversary can build data only in the compromise groups, not the entire system. The last scenario is intended for secure including capability. In previous scheme, the base station does not know how a lot of messages are aggregate from the decrypted aggregated result; leaking add up knowledge will suffer unkindly selective aggregation and frequent aggregation. In CDAMA, the base station accurately knows the number of mail aggregated to keep away from above attacks.

ARCHITECTURE DIAGRAM


Wireless sensor Networks
Transmission
Homomorphic encryptions
Absence of secure counting
Compromised sensor nodes
Single-application environments
Homomorphic public encryption system
CDA Scheme
CDAMA
Multiple points with different order
Multi-application Environments
Secure sensor Nodes
Secure counting

In WSN's, Accumulated broadcast carries large power cost for middle nodes. To add to the lifetime, tree-based or cluster networks force the midway nodes (a sub tree node or a cluster head) to perform aggregation to be aggregators (AG). After aggregation is completed, AGs would forward the results to next hop. The data can be aggregate via algebraic operation or arithmetical operations. For example, an AG can just forward the sum of arithmetical data received instead of forward all data to the next hop.

Adversary's abilities are categorize based on, overhear something on transmission information in a WSN, transfer forged data to any entity in a WSN, compromise secrets in SNs or AGs through capture them. Attacks are confidential into three categories to qualify the safety strength of a CDA scheme. In the first group A, an adversary needs to deduce the clandestine key. In category B, an adversary wants to send the forged messages to cheat the BS even though she does not be acquainted with the secret key. The last group C consists of three attacks and considers the collision of node compromise attacks. The first assault is the case of compromise an AG, and the previous two attacks are cases of compromise an SN.

In this module, various scheme are used for conceal infrastructure is specified. Privacy homomorphism encryption (PH) is an encryption method with homomorphism possessions. The homomorphism property implies that arithmetical operation on plaintexts can be implementing by manipulating the corresponding cipher texts. Conventional hop-by-hop aggregation schemes are insecure since an opponent is able to falsify aggregated results. To diminish this impact, PH schemes have be applied to WSNs. By PH schemes, SNs encrypt their sense readings and allow AGs to homomorphically collective their cipher texts with no decryption. It provides preservative and multiplicative homomorphism. Since, multiplicative property, base on the bilinear pairing, is much comfortable and incompetent for SNs, only the preservative homomorphism of is utilized.

IV. RESULT AND DISCUSSION

The Java Runtime Environment, or JRE, is the software required to run any application deployed on the Java Platform. End-users commonly use a JRE in software packages and Web browser plug-in. Sun also distributes a superset of the JRE called the Java 2 SDK (more commonly known as the JDK), which includes development tools such as the Java compiler, Java doc, Jar and debugger.

One of the unique advantages of the concept of a runtime engine is that errors (exceptions) should not 'crash' the system. Moreover, in runtime engine environments such as Java there exist tools that attach to the runtime engine and every time that an exception of interest occurs they record debugging information that existed in memory at the time the exception was thrown (stack and heap values).

V. CONCLUSION

In this paper, we have introduced, CDAMA, the first CDA scheme for a multi-application environment. It aggregates the cipher texts from distinct applications but not mixed. CDAMA is more secure for single-application environment when compared to other CDA schemes. When compromising attacks occur in WSNs, CDAMA mitigates the impact and reduces the damage to an acceptable condition. It is the first CDA scheme to support secure counting. The base station would know the exact number of messages aggregated, making selective or repeated aggregation attacks infeasible. The results performance evaluation shows that CDAMA is applicable on WSNs while the number of groups or applications is not large. In the future, we wish to apply CDAMA to realize aggregation query in Database-As-a-Service (DAS) model. The most important of all is that we do not have to consider the computation cost and the impact of compromising secret keys. Those drawbacks will no longer be issues in CDAMA.

VI. REFERENCES

1. Akyildiz .I, Su .W, Sankarasubramaniam .Y, and Cayirci .E (2002), "A Survey on Sensor Networks," IEEE Comm. Magazine, vol. 40, no. 8, pp. 102-114.
2. Cam .H, ¨ zdemir S.O, Nair .P, Muthuavinashiappan .D, and Sanli H.O (2006), "Energy-Efficient Secure Pattern Based Data Aggregation for Wireless Sensor Networks," Computer Comm., vol. 29, no. 4, pp. 446-455.
3. Girao. J, Westhoff .D, Schneider .M , N. Ltd, and Heidelberg .G (2005),"CDA: Concealed Data Aggregation for Reverse Multicast Traffic in Wireless Sensor Networks," Proc. IEEE Int'l Conf. Comm. (ICC '05), vol. 5.
4. Hu .L and Evans .D (2003), "Secure Aggregation for Wireless Networks," Proc. Symp. Application and the Internet Workshops, pp. 384-391.
5. Min .R and Chandrakasan .A, "Energy-Efficient Communication for Ad-Hoc Wireless Sensor Networks (2001)," Proc. Conf. Record of the

35th Asilomar Conf. Signals, Systems and Computers.

6. Perrig .A, Stankovic .J, and Wagner .D (2004), "Security in Wireless Sensor Networks," Comm. ACM, vol. 47, no. 6, pp. 53-57.

7. Przydatek .B, Song .D, and Perrig .A (2003), "SIA: Secure Information Aggregation in Sensor Networks," Proc. First Int'l Conf. Embedded Networked Sensor Systems, pp. 255-265.

8. I. Solis and K. Obraczka, "In-Network Aggregation Trade-offs for Data Collection in Wireless Sensor Networks," Int'l J. Sensor Networks, vol. 1, nos. 3/4, pp. 200-212, 2006.

9. F. Hu, X. Cao, and C. May, "Optimized Scheduling for Data Aggregation in Wireless Sensor Networks pp. 156- 168, 2005.

10. J. Li, A. Deshpande, and S. Khuller, "On Computing Compression Trees for Data Collection in Wireless Sensor Networks," pp. 2115-2123, 2010.