International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol. 3, Issue. 4, Jul - Aug. 2013 pp-2460-2463 ISSN: 2249-6645

Secure and Efficient Hierarchical Data Aggregation in Wireless Sensor Networks

Shaik Nagul Shareef[1], Syed Sadat Ali[2]
[1]*M. Tech, Nimra College of Engineering & Technology, Vijayawada, A.P., India.*
[2]*Assoc. Professor & Head, Dept.of CSE, Nimra College of Engineering & Technology, Vijayawada, A.P., India.*

***Abstract*:** *A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices that use sensor nodes to monitor physical or environmental conditions. These distributed autonomous devices, or nodes, combine with routers and a gateway to create a typical WSN system. The distributed sensor nodes communicate wirelessly to a central gateway, which provides a connection to the wired world where you can collect, process, analyze, and present your measurement data. Due to the broadcast nature of the transmission media they use, sensor networks are vulnerable to various security attacks, such as eavesdropping, jamming and node capture attacks. In this paper, we provide a solution for node capture attack. Node capture attacks result from the combination of active, passive and physical attacks by an intelligent adversary. In order to initialize or set up a node capture attack, the adversary will collect information about the WSN by eavesdropping on message exchanges, either local to a single adversarial device or throughout the network with the aid of a number of adversarial devices deployed throughout the network. Hence in order to securely aggregate data in a wireless sensor network, we must not only provide protection against eavesdroppers, but we should also prevent intermediate sensors from having access to the data.*

Keywords*: *Aggregation, Sensor node, Slicing, WSN.

I. INTRODUCTION

Wireless sensor networks (WSN) (Figure 1) are self organizing networks of small, battery powered sensors used to monitor the environment for events such as enemy troop movements in military, forest fires, pollutant levels. A large number of small, battery powered computing devices with built-in radio equipment are spread over the area to be monitored. Upon activation, these sensor nodes self-organize into a multi-hop network, which connects to the users via a powerful base station in order to achieve a common goal [1]. As each sensor surveys the area within its sensing range, the information is sent towards the base station along a multi- hop path. A sensor network is able to remotely cover a large sensing area since these low cost sensors organize into a multi-hop network without human assistance. Since sensor nodes are typically battery powered and a WSN contains thousands of sensors, replacing the batteries is not a possibility. In terms of energy usage, communication is much more expensive than any internal computations [2]. In data aggregation, intermediate results are calculated along the multi-hop path whenever two or more messages are routed along the same path. Depending on the routing structure, power savings may be by as much as eight times [3].

Security in sensor networks includes confidentiality, integrity and availability. Confidentiality in WSNs is accomplished by preventing outsiders from eavesdropping on transmissions. This is generally achieved by enciphering the relevant parts of a packet. Integrity in general means that the receiver is assured that the network packet was not tampered with or the message altered in some way. By ensuring the availability we mean that the data is available in a timely fashion so that it is useful to the user. Availability in WSNs is of great concern to the user of the network. Unfortunately, many existing security primitives can not be used in WSNs, either because the computing power of the sensors is too limited or the additional work created by the protocols causes excessive network traffic [4].

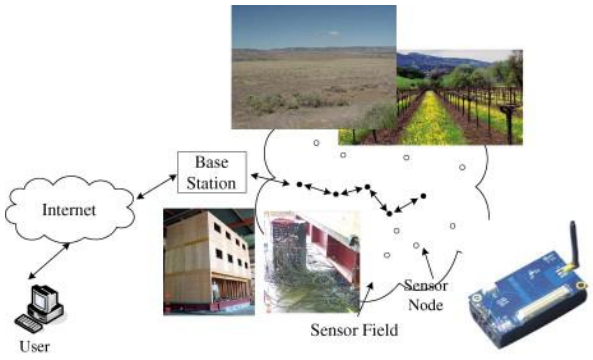

Figure 1 : Wireless sensor network example

Sensors in WSNs can become corrupted due to the environment such as water, wind or sand acting on the sensor. In hostile environments, a sensor may deliberately be corrupted by an attacker. A corrupted sensor may appear to participate in the mission of the network but falsify make sensor readings, improperly apply an aggregation function, exclude legitimate messages from the aggregate result or create a fictitious result. A sensor corrupted by an hacker may behave in this way in order to get the base station to accept an incorrect result that is favorable to the attacker. Hence in order to securely aggregate data in a sensor network, we must not only provide protection against eavesdroppers, but we should also prevent the intermediate sensors from having access to the data.

II. DATA AGGREGATION IN WSNS

In a typical WSN, a large number of sensor nodes collect application specific information from the environment and this information is transferred to a central base station where it is processed, analyzed, and used by the application. In these resource constrained networks, the general approach is to jointly process the data generated by different sensors while being forwarded toward the base station [5]. Such distributed in-network processing of data is generally called as data aggregation and involves combining the data that belong the same phenomenon. The main objective of hierarchical data aggregation is to increase the network lifetime by reducing the resource consumption of sensor nodes (such as battery energy and bandwidth). While increasing network lifetime, data aggregation protocols may degrade the important quality of service metrics in wireless sensor networks, such as data accuracy, latency, fault-tolerance, and security. Therefore, the design of an efficient data aggregation protocol is an inherently challenging task because the protocol designer must trade off between energy efficiency, data accuracy, fault-tolerance, latency, and security.

In order to achieve this trade off, data aggregation techniques are tightly coupled with how packets are routed through the sensor network. Hence, the architecture of the WSN plays a vital role in the performance of different data aggregation protocols. There are several protocols that allow routing and aggregation of network packets simultaneously. These protocols can be categorized into two parts: cluster-based data aggregation protocols and tree based data aggregation protocols. To reduce the latency due to tree based data aggregation, recent work on data aggregation process tends to group sensor nodes into clusters so that data are aggregated in each group for improved efficiency.

III. NODE CAPTURE ATTACK

WSNs are vulnerable to node capture attacks[6] because sensor nodes are usually deployed in unattended manner. Once attacker captures the sensor nodes, he can compromise them and launch various types of attacks with those compromised nodes. A straightforward strategy for sensor node compromise is to launch a node capture attack in which adversary physically captures all sensor nodes, removes them from the network, compromises and redeploys them in the network. After redeploying compromised nodes, he can mount a variety of attacks with the compromised nodes. For example, he can simply monitor a significant fraction of the network traffic that would pass through these vulnerable nodes. Alternatively, he could jam legitimate signals from benign nodes or inject falsified data to corrupt monitoring operation of the sensor nodes. A more aggressive attacker could undermine common sensor network protocols, including routing, cluster formation and data aggregation, thereby causing continual disruption to the network operations. Hence, node capture attacks are very dangerous and thus should be detected as quickly as possible to minimize the damage incurred by them.

IV. EXISTING SYSTEM

In Existing System, the aggregate data to be transmitted through sensor nodes, a security threat is originate by any node. So, that time attacker achieves full control over a sensor node through direct physical path in wireless sensor network. It makes to data loss and risk of data privacy. A typical sensor network consists of a large number of sensor nodes randomly deployed over a wide area. Sensor nodes are typically low cost hardware components with severe limitations on energy, memory and communication resources. The disadvantages of the existing system are:

1. Sensor nodes are exposed to maximum failures.
2. Sensor nodes which make use of the broadcast communication pattern and have severe bandwidth restraint.
3. Sensor nodes have inadequate amount of resources.

V. PROPOSED SYSTEM

In Proposed System, to avoid data loss initially sensor network is separated into different clusters each cluster is headed by an aggregator and directed connected to sink. So, this idea basically dispersed data processing measures to save the power and minimize the medium access layer contention in wireless sensor networks. It proposed the distinct Structure and Density Independent Group Based Key Management Protocol (DGKE) [7]. The protocol offers:

- A better secure communication,
- Secure data aggregation,
- Confidentiality and
- Resilience against node capture and
- Replication attacks using reduced resources.

A. Wireless Sensor Network

WSNs consist of numerous low cost, little devices and are in nature self organizing ad hoc systems. The job of the WSN is to monitor the physical environment, gather and transmit the information to other sink nodes. Generally, radio transmission ranges for the WSNs are in the orders of the magnitude that is lesser that of the geographical scope of the unbroken network. Hence, the transmission of the data is done from hop-by-hop to the sink in a multi-hop manner. Reducing the amount of the data to be relayed thereby reduces the consumption of energy in the network.

B. Hierarchical Secure Data Aggregation

Combine the data from various sources, redirect it with the removal of the redundancy and thereby reducing the number of transmissions and also saves energy. The inbuilt redundancy in the raw data gathered from various sensor nodes can be banned by the in-network data aggregation. Two securities in the data aggregation of sensor network is data Confidentiality: In particular, the fundamental security issue is the data privacy that protects the transmitted data which is

sensitive from the passive attacks like eavesdropping. The significance of the data confidentiality is in the hostile environment, where the wireless channel is more prone to eavesdropping attack. Though cryptography provides plenty of methods, such as the process related to complicated enciphering and deciphering, like modular multiplication of large numbers in public key based on cryptosystems, utilizes the sensor's power speedily. Data Integrity: It avoids the modification of the last aggregation value by the negotiating source nodes (aggregator nodes). Sensors can be without difficulty compromised because of the lack of the expensive tampering-resistant hardware. The otherwise hardware that has been used may not be reliable at all times. A compromised message is able to modify, forge and discard all messages.

C. Countering Node Capture Attacks

The process of getting hold of the sensors through a physical attack is termed as node capture attack. For example: uncovering the sensor node and adding wires in any place. This attack essentially differs from getting hold of a sensor via certain software bug. Since sensor nodes are typically supposed to operate the same software, specifically, the operating software which discovers the suitable bug permits the adversary to manage the entire sensor network. Distinctly, the node capture attacks can be set over the small segment of adequately large network. There are two types of node captures possible: Random node capture and Selective node capture. The following algorithm is used to detect node capture attacks.

Algorithm Node_Capture_Attack (node, aggregator, key, cluster, AGGadv)
{
// ui is a member node in cluster Cj where j = 1to n.
// Aj is the aggregator of the cluster Cj.
// AGGadv represents Aggregator Advertisement Message
// R1 is the first round of aggregation.
// TS1 is R1's respective time stamp.
// Aj possess a secret key (kjsec) which is shared with the sink.

$$A_j \xrightarrow{AGGadv} u_i$$

// In R1, the aggregator broadcasts the AGGadv to all the nodes.

$$u_i \xrightarrow{ACK} A_j$$

// ui sends acknowledgment (ACK) message to Aj.
// ACK = {wi, g} Where wi = node's ID, g = node's category. // based on ACK messages, the Aj selects c nodes (c<n) randomly.
Set Q = {u1, u2, …..uc}. // selected c nodes are represented by the set Q

$$A_j \xrightarrow{V} Q$$

V = [(w1, Kw1), (w2, Kw2), ……, (wc, Kwc)]
// the Aj broadcasts a set of unique values V to all nodes in Q. //V consists of the node ids of Q and their authentication key.
// Kwi denotes the authentication keys of the corresponding node wi.

$$u2 \xrightarrow{encr(1to(c-1))} u_3$$

X=1+2+…+C.
//X represents data which sliced into c pieces.
//assume u2 wants to send the data to any node .First u2 send encrypted data to nearest node u3.
//In c slices, one of them is kept inside that node itself.

$$X(1 \text{ to } (c\text{-}1)) \xrightarrow{decr(1 \text{ to } (c\text{-}1))} u3$$

//u3 waits for a time t, which assures that all slices of this round of aggregation are received. 1+2+…. +(c-1) =Sc
// sums up the received slices

$$u_3 \xrightarrow{encr(Sc)} Ai$$

//Sc is again encrypted with the authentication key of the respective node and sent to the Aj

$$Aj \xrightarrow{MAC(ED,TS)} Sink$$

// Aj aggregates and encrypts the data with the shared key kjsec and forwards it to towards sink.
//The message in the form MAC (ED, TS1) where TS1 = time stamp, ED = encrypted data.

If (TS1 → expires)
{
R1 → ends R2 → starts TS2→ begins
}
//The same procedure is repeated for R2 except that the set of nodes in Q is reselected with new
//set of authentication keys.
}

D. Slicing Technique

The Slicing technique is described using the slicing architecture shown in Figure 2. Consider the node 2 in below figure. When it wants to send data to its neighboring nodes, it slices the data "X" into 8 pieces (since network size u=8). It holds the one of the slices with it. The remaining slices are encrypted with their respective authentication keys and sent to rest of the sensor nodes.

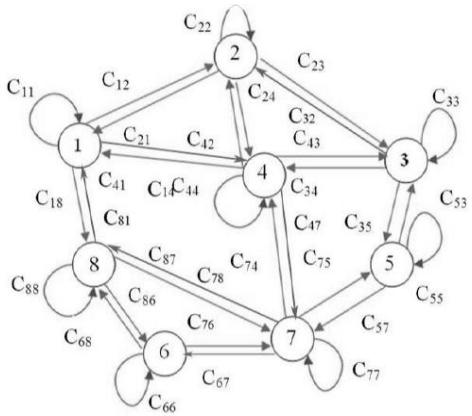

Figure 2: Slicing Technique

When the node 1 receives the encrypted data slice from node 2, then it decrypts the slice using its authentication key K1. Then Node 1 waits for reception of the rest of the slices until time "t". When "t" expires, the node 1 stops receiving the data slice. After complete decryption of the received slices, the node 1 sums them up along with the slice within it and this sum is represented as "S1".

$$S1 = C11 + C21 + C41 + C81$$

The node 1 encrypts "S1" with k1 and sent to the aggregator A1. The aggregator encrypts the data with a secret shared key (kjsec) and forwards it to the sink.

VI. CONCLUSION

WSNs are increasingly becoming the networks of choice in various industrial, medical and military applications, including remote plant control, health monitoring and target surveillance. Wireless sensor network consists of a huge number of tiny electromechanical sensor nodes that are capable of sensing, computing and communicating. Serious security threat is originated by node capture attacks in hierarchical data aggregation where a attacker achieves full control over a sensor node through direct physical access in wireless sensor networks. It makes a high risk of data privacy. In this propose, we propose a method for countering node capture attacks for hierarchical data aggregation in wireless sensor networks.

REFERENCES

[1] L. Clare, G. Pottie, and J. R. Agre, "Self-organizing distributed sensor networks," SPIE-The International Society for Optical Engineering, pp. 229–237, 1999.
[2] R. W. Heinzelman, J. Kulik, and H. Balakrishnan, "Adaptive protocols for information dissemination in wireless sensor networks," in MobiCom '99: Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking. ACM Press, 1999, pp. 174–185.
[3] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energyefficient communication protocol for wireless microsensor networks," in HICSS '00: Proceedings of the 33rd Hawaii International Conference on System Sciences-Volume 8. Washington, DC, USA: IEEE Computer Society, 2000, p. 8020.
[4] J. Albath and S. Madria, "Practical algorithm for data security (pads) in wireless sensor networks," in MobiDE '07: Proceedings of the 6th ACM international workshop on Data engineering for wireless and mobile access. New York, NY, USA: ACM Press, 2007, pp. 9–16.
[5] R. Rajagopalan, P.K. Varshney, Data aggregation techniques in sensor networks: a survey, IEEE Commun. Surveys Tutorials 8 (4) (2006).
[6] Conti, M., Pietro, R., Mancini, L., & Mei, A. (2008). Emergent Properties: Detection of the Node-capture Attack in Mobile Wireless Sensor Networks. In ACM WiSec, April 2008.
[7] K. Kifayat, M. Merabti, Q. Shi, D. Llewellyn-Jones, ―Group Based Secure Communication for Large-Scale Wireless Sensor Networks‖ , journal of information assurance and security, Vol 2, Issue 2, June 2007 .