Distributed Detection Of Safe Node Confine Attacks In Wireless Sensor Networks

Y.MAMATHA
MCA Student, Dept of MCA
DRK College of Engineering and Technology
Hyderabad, Andhra Pradesh, India

JYOTHSNA BANDREDDI
Assistant Professor, Dept of CSE
DRK College of Engineering and Technology
Hyderabad, Andhra Pradesh, India

Abstract: **In hierarchical data aggregation a severe safety hazard is originated by node confine attacks, where a hacker achieves full control over a sensor node through direct physical access in wireless sensor networks and it makes a high risk of data privacy. For hierarchical data aggregation in wireless sensor networks a securing node capture attacks is proposed in this paper. Each cluster is headed by an aggregator and the aggregators are directly connected to sink as network is separated into number of clusters. To the selected set of nodes in first round of data aggregation, the aggregator by identifying the detecting nodes selects a set of nodes randomly and broadcast an exclusive value which contains their validation keys. To relocate the data when any node within the group needs it transfers portion of data to other nodes in that group this is encrypted by individual validation keys. Each receiving node decrypts, sums up the portions and transfers the encrypted data to the aggregator. The data with the shared secret key of the sink and forwards it to the sink as the aggregator aggregates and encrypts. In the second round of aggregation the set of nodes is reselected with new set of authentication keys. The proposed technique resolves the security threat of node capture attacks is demonstrated by simulation results.**

Keywords: Safe Node, Confine Attacks, Wireless Sensor Networks, Data Privacy, Data Aggregation, Secret Key.

I. INTRODUCTION

The newest technology that has attained remarkable consideration from the research community is wireless sensor network. Sensor networks consist of various low price, modest devices and are in temperament self organizing ad hoc systems [1] [3] [4]. To monitor the physical environment, and to gather and transmit the information to other sink nodes is the job of the sensor network [2] [4]. Generally, for the sensor networks radio transmission range are in the orders of the magnitude that is lesser that of the geographical scope of the constant network [5] [6]. Hence, in a multi-hop manner the transmission of data is done from hop-by-hop to the sink. A huge number of tiny electromechanical sensor devices that are capable of sensing, computing and communicating are considered by wireless sensor network which is shown in fig 1[8] [9]. For gathering sensory information, these electromechanical sensor devices can be made use by capacity of temperature from a wide-ranging geographical area.

Many features of the wireless sensor networks have given increase to demanding problems. One of the fundamental discrete data processing measures to save the energy and reduce the average access layer conflict in wireless sensor networks is considered as data aggregation [7] [10]. For directing in the wireless sensor networks it is used as a significant pattern.

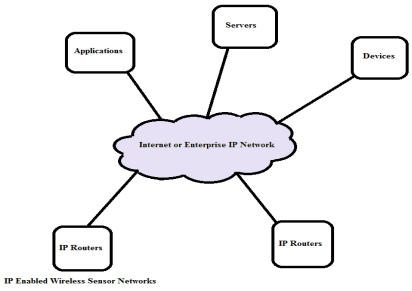

Fig 1: Sensor Network Security

II. HIERARCHICAL SECURITY IN THE AGGREGATION OF INFORMATION

By reducing the number of transmissions is the fundamental idea is to combine the data from diverse sources and transmit it with the removal of the redundancy and saves energy. From various sensors can be banned by the in-network data aggregation by the inbuilt redundancy in the raw data gathered [11] [12] [14]. In addition, to obtain application specific information these operations utilize raw materials. It is important for the network to preserve high incidence of the in-network data aggregation to conserve the energy in the system thereby maintaining longer lifetime in the network [13] [15]. The following are the issues that are connected to the safety in the data aggregation of WSN: Data Confidentiality: In particular, from passive attacks

like eavesdropping, the fundamental security issue is the data privacy that protects the transmitted data which is sensitive [16] [17]. The wireless channel is more prone to eavesdropping as the significance of the data confidentiality is in the hostile environment [18]. Data Integrity: By the negotiating source nodes or aggregator nodes it avoids the modification of the last aggregation value. Sensor nodes can be without complexity compromised because of the lack of the exclusive tampering-resistant hardware. A negotiation message is able to modify, counterfeit and discard the messages. Generally, for secure data aggregation in wireless sensor networks, two methods can be used. They are hop by hop encrypted data aggregation and end to end encrypted data aggregation.

III. NODE CONFINED ATTACKS:

The process of getting hold of the sensor node through a physical attack is termed as node confine attack. This attack effectively differs from getting hold of a sensor via certain software bug. The operating software which discovers the appropriate bug permits the challenger to handle the entire sensor network since sensors are typically supposed to operate the same software. Specifically, the node confine attacks can be situate over a small section of sufficiently large network. In node capture attack the merge of submissive, active and physical attacks by an intellectual opponent results. By overhearing something on message exchanges the adversary initializes an attack by gathering the data's about Wireless Sensor Networks (WSN). With the help of several adversarial devices organized in the entire network this is performed either locally to single adversarial device or via entire network. The challenger dynamically takes part in network protocols by inquiring the network regarding the information and injecting hateful information in the network along with unreceptive learning. To the attacker the above node captures varies in the key distribution information. During selective node capture attacks the attacker should minimum capture hundreds of sensor nodes. There is initiation of node capture attack where the challengers physically captures the sensor nodes and removes them and compromises and redistribute them in the network in sensor node compromise technique. It builds up a variety of attacks through compromised nodes by following the redistribution of the compromised nodes. With the formation of clusters routing and data aggregation the forceful attacker weakens the sensor network protocols and hence resulting in recurrent disruption of network operations. Therefore, for reducing the damages caused by them the node capture attacks are unsafe and need to be identified as soon as possible. The adversary attempts to tamper the node physically for extracting the secrets of the cryptography during the node capture attacks.

IV. RESULTS

Securing Node Capture Attacks for Hierarchical Data Aggregation system can be assessed by Network Simulator Version-2 simulation. In the beginning sensor nodes are located in square grid area by placing every sensor in a grid cell and the occurrence nodes move about the grid are organized to activate the measures. The performance of Securing Node Capture Attacks for Hierarchical Data Aggregation in Wireless Sensor Networks protocol can be compared for Data Aggregation protocol. The performance is measured according to the following measures such as Average end-to-end interruption in which the end-to-end-delay is averaged more than all existing data packets from the basis to the end. Average Packet Delivery Ratio: the ratio of the number of packets received and the total number of packets broadcasted. Average Energy is the common energy consumption of all nodes in transferring, receiving and forward process. Average Packet Loss is the average amount of packet dropped at each receiver. Throughput is the number of packets expected by the receiver.

V. CONCLUSION

For Hierarchical Data Aggregation in wireless sensor networks a securing node capture attacks is proposed in this paper. The aggregator identifies the detecting nodes selects a set of nodes randomly and broadcast a unique value which contains their authentication keys, to the selected set of nodes during first round of data aggregation. It sends slices of data to other nodes in that set when any node within the set wants to send the data, encrypted with their respective authentication keys. The encrypted data sends to the aggregator as each receiving node decrypts and sums up the slices. The aggregator aggregates and encrypts the information with the collective privacy key of the sink and forwards it to the sink. A new set of authentication keys are reselected by the set of nodes with in the second round of aggregation. The proposed approach rectifies the security threat of node capture attacks in hierarchical data aggregation is demonstrated by the simulation results.

REFERENCES

[1] Dorottya Vass, Attila Vidacs, ―Distributed Data Aggregation with Geographical Routing in Wireless Sensor Networks‖, Pervasive Services, IEEE International Conference on July 2007.

[2] Jukka Kohonen, ―Data Gathering in Sensor Networks‖, Helsinki Institute for Information Technology, Finland. Nov 2004.

[3] Gregory Hartl, Baochun Li, ―Loss Inference in Wireless Sensor Networks Based on Data Aggregation‖, IPSN 2004.

[4] Zhenzhen Ye, Alhussein A. Abouzeid and Jing Ai, ―Optimal Policies for Distributed Data Aggregation in Wireless Sensor Networks‖, Draft Infocom2007 Paper.

[5] Bhaskar Krishnamachari, Deborah Estrin and Stephen Wicker, ―The Impact of Data Aggregation in Wireless Sensor Networks‖, Proceedings of the 22nd International Conference on Distributed Computing Systems – 2002.

[6] Kai-Wei Fan, Sha Liu, and Prasun Sinha, ―Structure-free Data Aggregation in Sensor Networks‖, IEEE Transactions on Mobile Computing – 2007.

[7] Yingpeng Sang, Hong Shen, Yasushi Inoguchi, Yasuo Tan and Naixue Xiong, ―Secure Data Aggregation in Wireless Sensor Networks: A Survey‖, Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies, 2006.

[8] Zinaida Benenson, Nils Gedicke, Ossi Raivio, ―Realizing Robust User Authentication in Sensor Networks‖, Workshop on Real-World Wireless Sensor Networks (REALWSN05), June 2005, Stockholm, Sweden.

[9] Patrick Tague and Radha Poovendran, "Modeling Node Capture Attacks in Wireless Sensor Networks", 46th Annual Allerton Conference on Communication, Control, and Computing, September 2008.

[10] Jun-won Ho, ―Distributed Detection of Node Capture Attacks in Wireless Sensor Networks‖, InTech, Dec 2010

[11] Giacomo de Meulenaer, François-Xavier Standaert, ―Stealthy Compromise of Wireless Sensor Nodes with Power Analysis Attacks‖, MOBILIGHT 2010: 229-242

[12] Kui Ren, Wenjing Lou and Yanchao Zhang, ―LEDS: Providing Location-aware End-to-end Data Security in Wireless Sensor Networks‖, IEEE Transactions on Mobile Computing, Vol 7, Issue 5, pp 585 – 598, 2008.

[13] K. Kifayat, M. Merabti, Q. Shi, D. Llewellyn-Jones, ―Group Based Secure Communication for Large-Scale Wireless Sensor Networks‖, journal Bhoopathy V. and R.M.S. Parvathi / International Journal of Engineering Research and Applications (IJERA).

[14] Mr.V.Bhoopathy and R.M.S Parvathi, ―Energy Efficient Secure Data Aggregation Protocol for Wireless Sensor Networks‖, European Journal of Scientific Research, Vol.50 Issue 1, pp.48-58, 2011. [15] Mr.V.Bhoopathy and R.M.S Parvathi, ―Secure Authentication Technique for Data Aggregation in Wireless Sensor Networks‖ Journal of Computer Science, Vol. 8, Issue 2, pp 232-238, 2012.

[16] Yupeng Hu, Yaping Lin, Yonghe Liu, Weini Zeng, Hunan Univ., and Changsha, ―RAS:Robust authentication scheme for filtering false data in wireless sensor networks‖, 15th IEEE International Conference on Networks, (ICON), pp 200 – 205, 2007.

[17] Eldefrawy, M.H. Khan, M.K. Alghathbar, K, ―A key agreement algorithm with rekeying for wireless sensor networks using public key cryptography‖, International conference on anti-counterfeiting security and identification in communication (ASID), pp 1 – 6, 2010.

[18] Eitaro Kohno, Tomoyuki Ohta, Yoshiaki Kakuda, Masaki Aida: ―Improvement of Dependability against Node Capture Attacks for Wireless Sensor Networks‖, IEICE Transactions 94-D(1): 19-26 (2011)

BIOGRAPHY

Y Mamatha has completed B.Sc (Computers) from Vijetha Degree College, JNTU, Hyderabad and pursuing MCA in DRK College of Engineering & Technology, JNTUH, and Hyderabad. Her main research interest includes Wireless Sensor Networks & Computer Networks.

Jyothsna Bandreddi has completed B.Tech, Koneru Lakshamaiah College of Engineering,Working as Assistant professor in department of Computer science and engineering of DRK College of engineering and technology. . Her main research interest includes Wireless Sensor Networks & Computer Networks.

