IJARES/July 2014/Volume-2/Issue-7/1135-1140 **ISSN 2347- 9337**

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING AND SCIENCE

MANAGING HIERARCHICAL ACCUMULATION OF DATA IN WIRELESS SYSTEMS

N.Laxman[1], G.Krishna Veni[2]

[1]M.Tech Student, Dept of CSE, RRS College of Engineering & Technology, Muthangi (V), Patancheru (M), Hyderabad, T.S, India

[2]Assistant Professor, Dept of CSE, RRS College of Engineering & Technology, Muthangi (V), Patancheru (M), Hyderabad, T.S, India

ABSTRACT:

Sensor networks consist of various low price, modest devices and are in temperament self organizing ad hoc systems. During selective node capture attacks the attacker should minimum capture hundreds of sensor nodes. In support of protected data aggregation within wireless system, two methods are hop by hop encrypted aggregation data and continuous encrypted aggregation of data. A securing node capture attacks is introduced in support of Hierarchical Data Aggregation within wireless system. The node capture attacks are precarious and need to be recognized as soon as probable for dropping the damages caused by them.

Keywords: Wireless system, Data aggregation, Securing node capture attack, Self organizing ad hoc system.

1. INTRODUCTION:

A protection issue of wireless sensor network corresponds to node capture attack which leads to cooperation in the contact of a whole sensor network. 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. Sensor nodes can be without complexity compromised because of the lack of the exclusive tampering-resistant hardware [4]. Sensor set of connections consist of various low price, modest devices and are in temperament self organizing ad hoc systems. For gathering sensory information, the electromechanical sensor devices can be made use by capacity of temperature from a wide-ranging geographical area. One of the fundamental

discrete data handing out procedures to put aside energy and reduce the average access layer conflict in wireless sensor networks is considered as data aggregation. Normally, in wireless sensor networks shown in fig1 for protected data aggregation, two techniques can be used. They are hop by hop aggregation of encrypted data and continuous aggregation of encrypted data. In Hop-by-Hop encrypted data aggregation the encryption of the information is done by the sensing nodes and decryption by the aggregator nodes which summative the data and yet again encrypt the aggregation outcome [8]. From a variety of sensors are banned by aggregation of in-network data by intrinsic redundancy within raw data congregated. In meticulous, from passive attacks like eavesdropping, the basic security concern is the data confidentiality that defends transmitted information which is responsive. Wireless channel is additionally prone to eavesdropping while implication of data discretion is within hostile setting [1]. In sensor node compromise method, there is a commencement of node capture attack where the antagonist actually captures the sensor nodes, eliminate them, compromises and send them in the network. Subsequently the redeployment of the compromised nodes, it put together up a diversity of attacks all the way through compromised nodes. The forceful attacker deteriorate the sensor network protocols all along with the configuration of clusters, routing and data aggregation and for this reason resulting in recurrent interruption of network operations [11]. By reducing the number of transmissions is the fundamental idea is to combine the data from diverse sources and transmit it by elimination of redundancy also saves energy. In support of protected data aggregation within wireless system, two methods are hop by hop encrypted aggregation data and continuous encrypted aggregation of data [3]. By conferred source nodes otherwise aggregator nodes it circumvent alteration of preceding aggregation assessment. A negotiation message is able to modify, counterfeit and discard the messages.

2. METHODOLOGY:

In general, for the sensor networks radio transmission range are in extent of size that is slighter that of geographical extent of constant network performs monitoring of the physical environment, and broadcast data toward additional sink nodes [14]. A huge

number of tiny electromechanical sensor devices that are capable of sensing, computing and communicating are considered by wireless sensor network. In End to End encrypted data aggregation, the aggregator nodes in between does not include any decryption keys and can only carry out aggregation on the encrypted information. For an energy efficient secure data aggregation procedure for wireless sensor networks, we include the confirmation and protection to preserve the competence of the data aggregation [9]. The node capture attacks are precarious and need to be recognized as soon as probable for dropping the damages caused by them. For the duration of the node capture attacks, the adversary attempts to mess about the node physically for extracting the top secret of the cryptography. A securing node capture attacks is introduced in support of Hierarchical Data Aggregation within wireless system [7]. The aggregator recognizes the detecting nodes and selects a set of nodes arbitrarily and transmits an exceptional worth which include their verification keys, to chosen set of nodes during first round of data aggregation. It sends slices of information toward additional nodes in that set when any node within the set wants to send the data, encrypted with their respective authentication keys [2]. 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 concerning sink and promote it toward sink. A new set of authentication keys are reselected by the set of nodes with in the second round of aggregation. The introduced advance resolve the safety hazard concerning node capture attacks in hierarchical data aggregation is demonstrated by the simulation results. The data with the common undisclosed key of sink and ahead it toward sink as the aggregator aggregates and encrypts [16]. In subsequently round of aggregation the set of nodes is reselected with latest set of confirmation keys. The introduced technique determines the safety threat of node capture attacks is verified by simulation results. Based on the protection architecture of the network, this type of attack is highly vicious and in addition fallout in significant insider attacks. Secure authentication technique for data aggregation in wireless sensor networks, for the duration of first round of data aggregation, the aggregator upon

recognizing the detecting nodes go for a set of nodes at random and transmit a exceptional value which contains their verification keys, to the selected set of nodes [12]. as soon as any node inside the set wants to send the data, it sends slices of information to additional nodes in that set, encrypted with their particular confirmation keys. On every occasion a sensor node wants to send data to an additional node; initial the sensor node encrypts the information by means of a key and sends it to the aggregator [5] The safety problem of wireless sensor network such as node capture attacks is not taken into deliberation. This node capture attack is destructive for network message in network data aggregation, routing and so on.

3. AN OVERVIEW OF APPROVAL OF SENSOR NODE BY A PHYSICAL AGGRESSION:

The newest technology that has attained extraordinary 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. The procedure of entering sensor node all the way through a physical attack is named as node confine attack and is effectively is at variance from obtaining a sensor by means of convinced software bug [15]. The adversary attempts to tamper the node physically for extracting the secrets of the cryptography during the node capture attacks. 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 and builds up a variety of attacks through compromised nodes by following the redistribution of the compromised nodes [10]. During selective node capture attacks the attacker should minimum capture hundreds of sensor nodes. In support of reducing the damages caused by them the node capture attacks are unsafe and need to be identified as soon as possible. The node confine attacks can be situated over a small section of sufficiently large network [6]. In node capture attack the merge of submissive, active and physical attacks by an intellectual opponent results. The operating software which discovers the appropriate bug permits the challenger to handle the entire sensor network in view of the fact that sensors are naturally believed to role identical software. 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 [13]. To the attacker the above node captures varies in the key distribution information. 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.

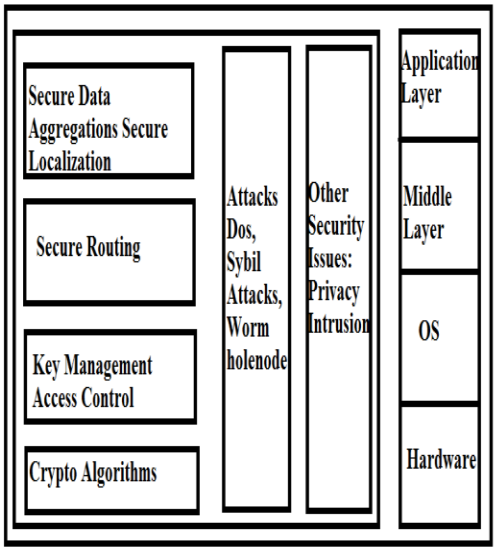

Fig 1: Wireless Sensor Network Security Architecture.

4. CONCLUSION:

The newest technology that has attained extraordinary consideration from the research community is wireless sensor network. A protection issue of wireless sensor network corresponds to node capture attack which leads to cooperation in the contact of a whole sensor network. In sensor node compromise method, there is a commencement of node capture attack where the antagonist actually captures the sensor nodes, eliminate them, compromises and send them in the network. For an energy efficient secure data aggregation procedure for wireless sensor networks, we include the confirmation and protection to preserve the competence of the data aggregation. The introduced advance resolves the safety hazard concerning node capture attacks in hierarchical data aggregation. 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. Secure Authentication Technique for Data Aggregation in Wireless Sensor Networks, for the duration of first round of data aggregation, the aggregator upon recognizing the detecting nodes go for a set of nodes at random and transmit

a exceptional value which contains their verification keys, to the selected set of nodes.

REFERENCES:

[1] 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.

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

[3] Mauro Conti, Roberto Di Pietro, Luigi V. Mancini, Alessandro Mei, ―Emergent properties: detection of the node-capture attack in mobile wireless sensor networks‖, In Proceedings of WISEC'2008. pp.214~219.

[4] "Securing Node Capture Attacks for Hierarchical Data Aggregation in Wireless Sensor Networks", Bhoopathy, V. and R.M.S. Parvathi, 2012

[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] Ka-Shun Hung; Chun-Fai Law; King-Shan Lui; Yu-Kwong Kwok, ― On Attack-Resilient Wireless Sensor Networks with Novel Recovery Strategies‖, IEEE conference on wireless communication and networking conference(WCNC), pp1 – 6, 2009.

[7] 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.

[8] 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.

[9] 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).

[10] 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.

[11] 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.

[12] 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.

[13] 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)

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

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

[16] 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.