ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Analysis of Secure In-Network Aggregation for Anomaly Detection in Wireless Sensor Networks

Arthi.A[1]

PG Scholar, Department of ECE, SNS College of Technology, Chennai Anna university, Tamil Nadu, India[1]

ABSTRACT: Secure in-network aggregation in wireless sensor networks is a necessary and challenging task. Secure in-network aggregation refers to acquiring the sensed data from the sensors and transmitting the sensed information to the gateway node. Integration of system monitoring modules and intrusion detection modules are proposed in WSN. An Invariant extended Kalman filter based mechanism is used to detect false injected data in case of non-linear systems possessing symmetries. This task is challenging because of potential high packet loss rate, harsh environment, and sensing uncertainty. The main objective of secure in-network aggregation is to reduce the packet loss rate and small power consumption. An algorithm for combining cumulative summation and generalized likelihood ratio is used to increase detection sensitivity. To overcome the limitations of local detection mechanisms, our proposed local detection approaches work together with the system monitoring module to differentiate between malicious events and emergency events.

KEYWORDS: Extended Kalman Filter, Invariant Extended Kalman Filter, system monitoring module, Intrusion detection module.

I. INTRODUCTION

Wireless sensor networks can be considered as a network of nodes that can sense the environment and communicate the information gathered from the monitored field through wireless links and the data is forwarded possibly via multiple hops relaying to a sink or to other networks through a gateway. Nodes typically have stringent energy limitations, which make them more failure-prone. WSNs usually use a low duty cycle where nodes are in sleeping mode most of time and only wake up asynchronously, to conserve energy and increase the life time of the network. In a large sensor network, in-network data aggregation significantly reduces the amount of communication and energyconsumption since it uses optimal path to send information to the destination. Anomaly detection can be used to detect these abnormal behaviours. It has been used for a long time in various applications to detect and remove anomalous data or activities. Any observation that significantly differs from the normal pattern can be considered as abnormal behaviour and this will vary between applications and system properties.

II. RELATED WORK

Bo Sun ,Xuemei Shan and Kui Wu proposed that secure in-network aggregation in wireless sensor networks (WSNs) is a necessary and challenging task. Integration of system monitoring modules and Intrusion detection modules are proposed in the context of WSNs. Extended Kalman filter (EKF) based mechanism to detect false injected data. Specifically, by monitoring behaviors of its neighbors and using EKF to predict their future states. An algorithm for combining cumulative summation and generalized likelihood ratio is used to increase detection sensitivity. EKF is used to address various uncertainties in WSNs and create an effective local detection mechanism. INTRUSION DETECTION MODULES (IDM) can work together with SYSTEM MONITORING MODULES (SMM) in order to differentiate between malicious events and emergency events.

K. Wu, D. Dreef, B. Sun, and Y. Xiao In-network data aggregation is an essential operation to reduce energy consumption in large-scale wireless sensor networks. First, it introduces some topological constraints when building a Secure Aggregation nee (SAT), which facilitates the monitoring of the behavior of each aggregation sensor node. Second, when the aggregated values from an aggregation node are in doubt, a weighted voting scheme is proposed to

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

decide finally whether the aggregation node is properly behaving or is cheating.Third, if a misbehaving node is detected, a local recovery scheme is presented to re-build SAT so that the misbehaving node is excluded from the aggregation tree. Since no cryptographic operations are required when all nodes work. This method is lightweight. Since no centralised operations are needed at the base station, this method also scales very well.

ANOMALY DETECTION:

Anomaly detection can be used to detect these abnormal behaviours. It has been used for a long time in various applications to detect and remove anomalous data or activities .[1] Any observation that significantly differs from the normal pattern can be considered as abnormal behaviour and this will vary between applications and system properties. It can also be very difficult to obtain the normal behaviour model of a distributed system like WSN.

DATA AGGREGATION:

Data aggregation in Wireless Sensor Network refers to acquiring the sensed data from the sensors to the gateway node. Data aggregation plays a vital role in Wireless Sensor Networks. since the aggregation schemes followed here involve in reducing the amount of power consumed during data transmission between the sensor nodes.

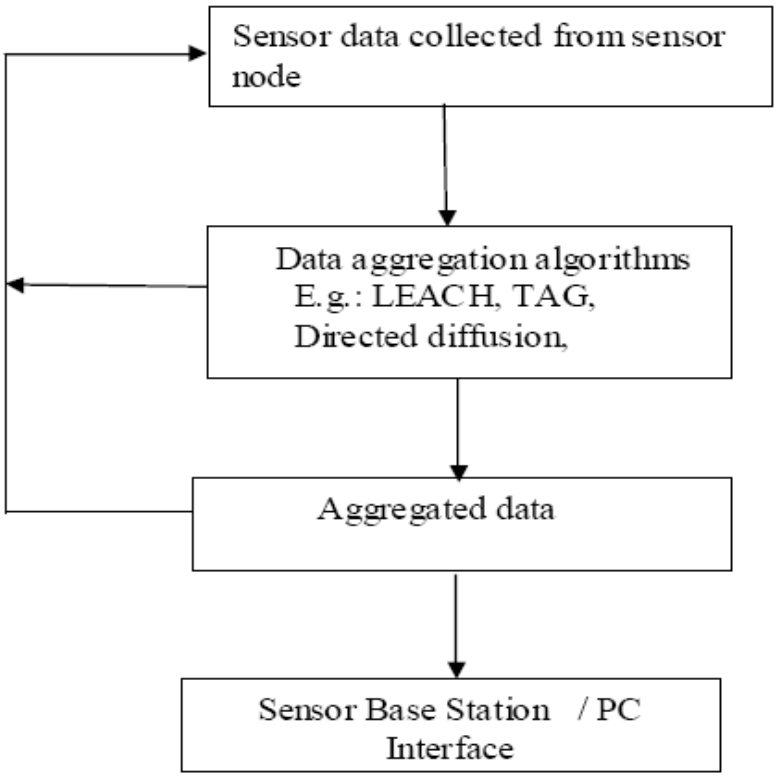

Fig. ARCHITECTURE OF DATA AGGREGATION

IN NETWORK AGGREGATION:

In-network aggregation is a global process of gathering and routing information through a multi-hop network, processing data at intermediate nodes with the objective of reducing resource consumption (in particular energy), thereby increasing network lifetime.[2] This method reduces the communication overhead.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

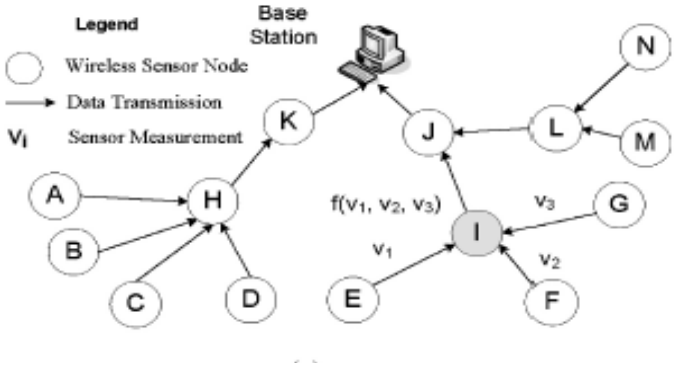

Fig. EXAMPLE OF AGGREGATION TREE

Aggregation tree is built and A,B,C, and D perform sensing tasks, obtain values and transmit them to their parent node H. H aggregates the received values from A,B,C, and D, and transmits the aggregated value further up to node K. The same is true for operation (E, F,G) → I → J and operation (M,N) → L → J. These aggregation operations are performed based on the established parent–child relationship, where the base station collects all these data and, if necessary, can transmit them across the Internet.

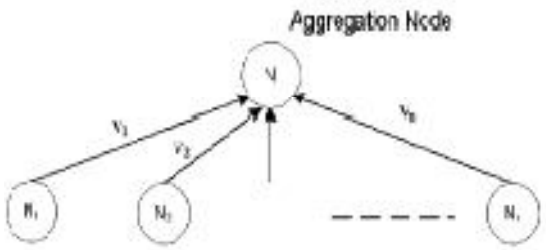

Fig. AGGREGATION MODEL

For the purpose of saving node energy, there have been extensive research efforts on various kinds of sensor node scheduling policies, in which a minimum number of nodes remain awake to satisfy a certain degree of coverage. Therefore, an assumption is made that the sensor nodes may go to sleep and the necessary sensor nodes could be woken up anytime once required.

INTRUSION DETECTION MODULE AND SYATEM MONITORING MODULE:

Secure in-network aggregation protocol is equipped with two modules: INTRUSION DETECTION MODULES (IDM) and SYSTEM MONITORING MODULES (SMM).The functionality of the IDM is to detect whether monitored nodes are malicious insider nodes, while the functionality of the SMM is to monitor important emergency events.SMM is a necessary component for most of WSN applications. IDM and SMM need to be integrated with each other to work effectively.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

INVARIANT EXTENDED KALMAN FILTER:

INVARIANT EXTENDED KALMAN FILTER (IEKF) is a new version of the extended Kalman filter (EKF) for nonlinear systems possessing symmetries or Invariances. It combines the advantages of both the EKF and the recently introduced symmetry-preserving filters. Instead of using a linear correction term based on a linear output error, it uses a geometrically adapted correction term based on an invariant output error; in the same way the gain matrix is not updated from a linear state error, but from an invariant state error. The main benefit is that the gain and covariance equations converge to constant values on a much bigger set of trajectories than equilibrium points than is the case for the EKF, which results in a better convergence of the estimation.Invariant EKF and CUSUM GLR to identify the adversary when majority of its neighbors are compromised. High packet loss rate is reduced. Time synchronization is achieved between parent node and child node.Robust and effective intrusion detection for secure in-network aggregation. Energy consumption is reduced.

CUMMULATIVE SUMMATION AND GENERALIZED LIKELIHOOD RATIO:

An algorithm of combining cumulative summation (CUSUM) and generalized likelihood ratio (GLR) is used toincrease detection sensitivity when malicious values have small deviations. To decrease the overhead, The computation is simplified and made the CUSUM GLR algorithm suitable for sensor nodes. CUSUM and GLR utilizes the cumulative sum of the deviations between measured values and estimated values.[3]IDM and SMM should work together to provide intrusion detection capabilities for WSN.

III. CONCLUSION

Secure In-network aggregation aggregates the results from sensor nodes and transmits the aggregated information to the base station. Secure in-network reduces the communication overhead and saves energy. Invariant Extended Kalman Filter is used to detect the false injected data. The functionality of the IDM is to detect whether monitored nodes are malicious insider nodes, while the functionality of the SMM is to monitor important emergency events. Cumulative summation and generalized likelihood ratio is used to increase the detection sensitivity

.

REFERENCES

1.Anomaly Detection Based Secure In-NetworkAggregation for Wireless Sensor Networks. Bo Sun, Member, IEEE, Xuemei Shan, Kui Wu, Senior Member, IEEE, and Yang Xiao, Senior Member, IEEE.

2.S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An interleaved hop-by-hop authentication scheme for filtering false data injection in sensor networks," in Proc. IEEE Symp. Security Privacy, May 2004.

3.Z. Yu and Y. Guan, "A dynamic en-route scheme for filtering false data injection in wireless sensor networks," in Proc. IEEE INFOCOM, Apr.2006, pp. 1–12.

4.K. Wu, D. Dreef, B. Sun, and Y. Xiao, "Secure data aggregation without persistent cryptographic operations in wireless sensor networks," Elsevier Ad Hoc Networks .

5. L. Hu and D. Evans, "Secure aggregation for wireless networks," in Proc. Workshop Security Assurance Ad Hoc Network., Jan. 2003