Efficient Filtering and Location Detection against Insider Attacks in WSN

Jeena Elezabeth Cheriyan, S. Sathees Babu and K. Balasubadra

Abstract--- *Improving the security in wireless sensor networks(WSNs) is a necessary and challenging task in recent days. There are several techniques proposed for attaining security in data aggregation. Among those system monitoring modules(SMM) and intrusion detection modules(IDM) are the two techniques which perform the detection of external and internal threats of WSNs. This work illustrates how local detection approaches work together with the SMM to differentiate between internally malicious events and emergency events to overcome the limitations of local detection mechanisms. Preserving privacy is also an important concern when data aggregation takes place in military applications. An Extended Kalman Filter(EKF) based mechanism is used to detect false injected data. Specifically by monitoring behaviours of its neighbours and using EKF to predict future states. Each node aims at setting up a normal range of neighbours' future transmitted aggregated values. An algorithm combining cumulative summation and generalized likelihood ratio(GLR) algorithms are used to create effective intrusion detection.*

Keywords--- *System Monitoring Modules (SMM), Extended Kalman Filter (EKF), Cumulative Summation(CUSUM), Generalized Likelihood Ratio(GLR)*

I. INTRODUCTION

A WIRELESS sensor network is a group of sensor nodes which communicate with each other and meant to both monitor conditions and collect values at different locations. The parameters which are commonly monitored are variation in temperature, humidity conditions, pressure, wind direction etc. A sensor network consists of sensor nodes which act as detecting stations that are portable and small.

In a typical WSN, a number of sensor nodes are deployed in an area of interest and they self-organize to form a network. The values sensed by sensor nodes are collected by a sink or base station BS (which is computationally more powerful and secure than sensor nodes) for further processing. For typical applications where the sink is only interested in some kind of aggregate value such as the average of all sensed values, the aggregate value is collected via an in-network data aggregation process (for reducing energy consumption) in which partial aggregate values are combined at intermediate nodes en route to the sink. This process is realized by constructing a spanning tree among sensor nodes with the sink directly connected to the central sensor node, and each sensor node aggregates its incoming data with its own sensed value, and then sends the result to its parent node in the tree.

In this work, we investigate internal attacks [2] of wireless sensor networks. Whenever a sensor node gets attacked by intruder, all its data become accessible to attackers and thus leaves the network weak. System Monitoring Modules (SMM) is a necessary component for most of WSN applications. To enhance security in WSNs, Intrusion Detection Modules(IDM) and SMM has to be integrated with each other to for its effective work. Local detection alone is not desirable because available information in each node is very less. Since sensor nodes face failure it is tiring task to differentiate between emergency events sent by good nodes and malicious events. In this work, whenever IDM and SMM detect some malicious events, they need to request for more sensor nodes around the events to make a final decision.

The false injected data is detected using EKF (Extended Kalman Filter) mechanism. This is done by behavior of its nearby nodes which gets monitored and using EKF to predict next possible states. A series of neighbor nodes' expected values in the succeeding states is being stored by each node. Rate of packet loss, noisy environment, sensing inaccuracy, time asynchrony between children and parent nodes make this task tedious. A state space-model is utilized in EKF based mechanism in WSN nodes. Utilizing a threshold-based mechanism, an overheard value and the locally computed normal range is compared to decide whether there is notable difference. Then analysis of how to decide the thresholds under different functions for aggregation(average of aggregation, sum, max, and min etc) is done. A combined algorithm with cumulative summation (CUSUM) and generalized likelihood ratio (GLR) [1] is used to create effective location detection in WSNs which utilizes the cumulative sum of the deviations between measured values and estimated value.

II. RELATED WORK

There are many research efforts that address security issues in WSN. But the problem of internal threats was addressed by Zhang and Jajodia [2].This protocol might be vulnerable if both a child node and its parent node are compromised. An aggregate-commit-prove framework by Przydatek et al., is also a related work. Another work by Chan et al. an optimally secure aggregation scheme was presented for multiple malicious nodes and arbitrary topologies.

Jeena Elezabeth Cheriyan, M.E, Student, Dept of CSE, PSNACET, Dindigul, India. E-mail: jeenacherian88@gmail.com

S.Sathees Babu, Associate Professor, Dept of CSE, PSNACET, Dindigul, India. E-mail: ssbabu@psnacet.edu.in

K.BalaSubadra, Professor, Dept. of IT, R.M.D College of Engineering and Technology, Chennai, India. E-mail: balasubadra@yahoo.com

Annapoorna Rao, Priyanka Singh, Shruthi R and Syeda S. Rubbani [3] explained a defending mechanism on insider attacks in wsn. The work by Wagner used statistical estimation for more resilient aggregation schemes against malicious data injection attack in which a mathematical framework is presented to formally evaluate security of different aggregation algorithm. Aggregation free from attacks in wireless sensor networks is explained in [2], but no detailed simulations and experiments are carried out. Staddon et al., [8] proposed an idea about tracing failed nodes in wsn. There are some resilient aggregation algorithms aiming to increase the likelihood of accurate results when WSNs are prone to message loss and node failure [14]. Also, a number of proposed protocols aim to ensure the privacy of data [3]–[5] in WSNs.

Several protocols are proposed to filter false data in WSNs. Liu et al., [11] discussed about insider attacker detection in wsn. Generally, they utilize different key distribution mechanisms to develop filtering capabilities. In these related work efforts, different sensing reports are validated by message authentication codes along the way to the sink. The sink can further filter out remaining false reports that escape the filtering en route. There is also some research work using statistical approaches like a Bayesian algorithm to deal with the possibility of measurement faults in sensors. These efforts have become a great support for applications, including target finding, data query, and fault data detection. Detection using kalman filter and cumulative summation mechanisms have also been widely used in many applications. For example, in the context of WSNs, KF was used to enable accurate target tracking [14]. Unlike above techniques, proposed scheme aims at addressing internal threats using effective algorithms mentioned above. KF and CUSUM have not yet been applied to secure WSN aggregation services. This paper relies on future values of node in succeeding states with the help of nearby nodes and can complement existing mechanisms to prevent attacks in network.

III. Module Description

An aggregation tree is built first to show child parent relationship in network.. In Fig. 1(a), A,B,C, and D perform sensing tasks, obtain values and transmit them to their parent node H. The received values from A,B,C, and D is aggregated, and transmits the aggregated value further up to node *K*. The same operation is done at (E, F, G) → I → J and operation (M,N) → L → J.

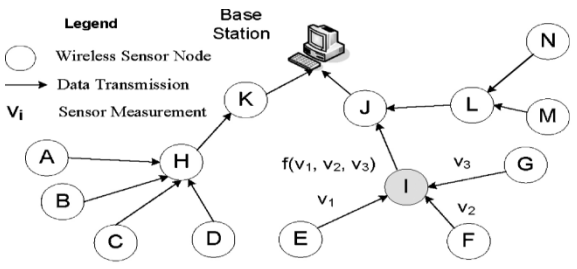

Fig. 1: Wireless Sensor Network- Aggregation Model

When one node, e.g., F in Fig. 1(a), is within the radio transmission range of another node, e.g., I, node F can overhear node I's transmissions. This facilitates our proposed neighbor monitoring mechanisms. 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, we assume that sensor nodes may go to sleep.

A sensor node when compromised by an adversary, this adversary can take full control of the compromised node. It may inject falsified data readings or nonexistent readings into the WSN. It is assumed that data that is falsified is transmitted by a compromised node is very different from the state (the actual value, for example, the actual monitored average temperature) so that falsified data can effectively disrupt aggregation operations. Hence a security model is proposed which consists of 2 modules, IDM and SMM. The IDM is used to detect whether monitored nodes are malicious nodes or not, while the functionality of SMM is to monitor emergency events. Using IDM, when node A raises an alert on node B because of an event E , A can further initiate investigation on with the help of SMM. Specifically, can wake up relevant sensor nodes around B and request their opinions about E. If the majority of sensor nodes think that E could happen, A can make a decision that E is triggered by some emergency event. Otherwise, A can suspect that E is malicious.

IV. Extended Kalman Filter Detection

State represents an actual value to be measured. State at a given instant of time is characterized by instantaneous values of an attribute of interest. For example , actual temperature monitored by WSNs. In the state space model, actual aggregated values form a dynamic process, and a process model given by,

$$x_{k+1} = f(x_k) + w_k \qquad (1)$$

where x_k represents the actual value at time t_k. F is a function relating x_{k+1} to x_k and w_k is the process noise at time t_k.

Measurement model is given by,

$$z_k = H(x_k) + v_k = x_k + v_k \qquad (2)$$

where zk is the measured value at time tk. H is the function relating xk to zk the function relating x_k to z_k and v_k is the measurement noise at time t_k.

System equations is given by,

$$\hat{x}^{-}_{k+1} = \mathrm{F}(\hat{x}^{+}_{k}) \qquad (3)$$

Basically, at time t_k, to predict the actual value x_{k+1}, a node needs two values:

- the a priori estimate $\hat{x}^{-}_{k+1}$ which can be obtained based on (3).
- the measured value z_{k+1} that can be promiscuously overheard. EKF can provide a relatively accurate prediction of neighbors' future aggregated values.

Algorithm 1 EKF based local detection algorithm

Assumption Node X can overhear node Y's transmission. X thinks that Y is a normal node at and before time t_k .

Input z_{k+1} transmitted by node B and overheard by node A.

Output whether A raises an alert on z_{k+1}

1: At time t_k, A computes $\hat{x}_k^+$ ($\hat{x}_k^-$ is stored in node A);
2. A computes $\hat{x}_{k+1}^-$ based on $\hat{x}_k^+$ using (3);
3. A computes Diff = $|\hat{x}_{k+1}^- - z_{k+1}|$;
4. if (Δ < Diff) then
5. A raises an alert on B;
6. else
7. A thinks that B functions normally;
8.end if

Now we present EKF based location detection algorithm. A sensor node monitors its neighbor's behavior and establishes a normal range of the neighbor's future aggregated values. The creation of the normal range is based on values using EKF. An alert can be raised if the monitored value lies outside of the predicted normal range. In the algorithm A's role is to decide whether z_{k+1} is abnormal or not. Node A can overhear Node B's transmission z_{k+1} at time t_{k+1}. After estimating $\hat{x}_k^+$ at time t_k, a can predict node B's transmitted value based $\hat{x}_{k+1}^-$ at time t_{k+1} based on (3). At time t_{k+1} , A overhears B's transmitted value z_{k+1} and compares $\hat{x}_{k+1}^-$ with z_{k+1} to decide whether B is acting normally or not. If the difference between $\hat{x}_{k+1}^-$ and z_{k+1} is larger than Δ, a predefined threshold, A then raises an alert on B. Else, A thinks that B functions normally.

V. CUSUM GLR Based Local Detection

An EKF based approach at times neglects the information given by the entire sequence of measured values. For example in Algorithm 1 if an attacker continuously injects $z_{k+1}$with small deviations, this leads to a small Diff. A relatively large Δ can make an EKF based approach insensitive to these kinds of attacks because this approach only uses information available at a previous time instant.

An algorithm combining CUSUM and GLR[1] is used which utilizes the cumulative sum of deviations between measured values and estimated values.

Algorithm 2 CUSUM GLR based local detection algorithm

Assumption Node A can overhear node B's transmission. A thinks that B is a normal node at and before time tk

Input A sequence of z_{k+1} transmitted by node B and overheard by node A

Output Whether node A raises an alert on z_k

1: Compute $y_k = z_k - \hat{x}_k^-$ at time t_k.
2. Compute $\hat{\mu}_1 = \frac{1}{w}\sum_{i=k-w+1}^{k} y_i$ when k $\geq w-1$
3. $S_N = \frac{b}{\sigma}\sum_{i=0}^{N}\left(yi - \mu_0 - \frac{v}{2}\right) = \frac{b}{\sigma}\sum_{i=0}^{N}\left(yi - \frac{v}{2}\right)$
4. if $(S_N > h)$ $then$
5. A raises alert on B;
6. else
7. A thinks that B functions normally;
8. end if

VI. Experimental Evaluation

EKF and CUSUM GLR algorithms are implemented using network simulator, ns2. The purpose of the simulation is to filter out the malicious node and to find out whether an alert raised is genuine or not. The node size is set to 100 nodes. This to monitor a small geographic area for temperature values. Each node of the network is equipped with a 2 Mbps 802.11 radio with an omnidirectional antenna. Nodes will have 250m as the transmission range and 550m as their sensing range. The two-ray radio propagation model is used. The interference queue length is chosen as 50 packets in each node. We take We take the packet size as 1024 bytes at a packet rate of 8 packets per second. The minimum speed is taken as 5 m/s whereas the maximum speed is 8m/s. We collect data from the simulation run of 100 seconds. In EKF algorithm, the parameters used are diff, a predefined threshold value is calculated using sum of aggregations or min, max value of aggregation. v_k is the measurement noise and w_k is the process noise at time t_k, priori and posteriori values already set in the node.

The parameters used in CUSUM GLR algorithm are s_k, the ratio of observed values, s_N, the cumulative sum of deviations. h is the predefined threshold value, y_k is the observed value at t_k and $\hat{\mu}_1$ is the mean of observed values. This is used for comparing observed value with threshold value. The performance of both the algorithms can be evaluated by comparing the throughput. The graph shown below is plotted with throughput in the y-axis and number of nodes in x-axis. As the number of nodes increases, effective filtering of malicious nodes can be made possible.

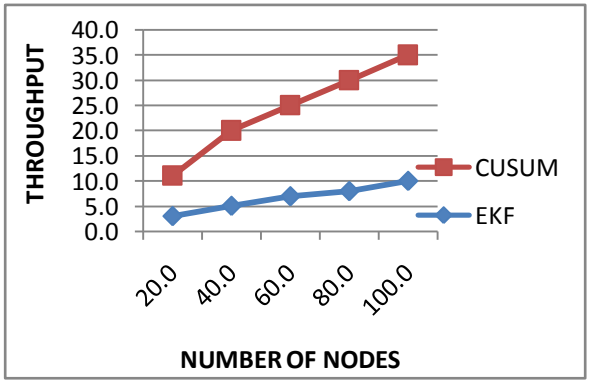

Fig. 2: Performance Chart based on EKF and CUSUM Algorithms

VII. Conclusion

Network security plays a significant role in technological advancement. The proposed model has a potential to be used as an effective and strong solution against the internal attacks. The filtering of false data and location detection of malicious nodes can be successfully detected even if the adversary injects small amount of data into the network.

As a future work, a timing control algorithm can be incorporated in this work so that sink node will be open for particular time and thus it can prevent false incoming signals.

REFERENCES

[1] Bo Sun, Member, IEEE, Xuemei Shan, Kui Wu, Senior Member, IEEE, and Yang Xiao, Senior Member, IEEE, "Anomaly Detection Based Secure In-Network Aggregation for Wireless Sensor Networks" in IEEE SYSTEMS JOURNAL, VOL. 7, NO. 1, MARCH 2013.

[2] Lei Zhang, Honggang Zhang, Mauro Conti, Roberto Di Pietro, Sushil Jajodia, Luigi Vincenzo Mancini "Preserving privacy against external and internal threats in WSN data aggregation", in Telecommun Syst (2013) 52:2163–2176 DOI 10.1007/s11235-011-9539-8.

[3] Annapoorna Rao, Priyanka Singh, Shruthi R and Syeda S. Rubbani, "Defending mechanism to secure nodes from internal attack in wsn" in International Conference on Advances in Computer and Electrical Engineering Nov. 17-18, 2012 Manila (Philippines).

[4] Ahmad Ababnah, Balasubramaniam Naatarajan, "Optimal control based strategy for sensor deployment." IEEE Tran. On Systems, Man, and cybernetics, Part A: Systems and Humans, vol. 41, no. 1 Jan. 2011.

[5] 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, pp. 260–272, May 2004.

[6] Y. Zhang, W. Liu, W. Lou, Y. Fang, "Location-based compromise tolerant security mechanisms for wireless sensor networks," IEEE Journal on Selected Areas in Communications, Special Issue on Security in Wireless Ad Hoc Networks, Vol. 24, No. 2, pp. 247-260, February 2006.

[7] K. Ren, W. Lou, Y. Zhang, "LEDS: providing location-aware end-to end data security in wireless sensor networks," in IEEE INFOCOM 2006, Barcelona, Spain, April 2006.

[8] J. Staddon, D. Balfanz, and G. Durfee, "Efficient tracing of failed nodes in sensor networks," in WSNA 2002, pp. 122-130, Atlanta, USA.

[9] Ochirkhand Erdene Ochir, Marine Minier, Fabrice Valois, and Apostolos Kountouris, "Resiliency of Wireless Sensor Networks: Definitions and Analyses", 2010 17th International Conference on Telecommunications, pp828-835.

[10] Hung-Min Sun, Chien-Ming Che, and Ying-Chu Hsiao, "An efficient countermeasure to the selective forwarding attack in wireless sensor network," IEEE Region 10 Conference (TENCON), 2007, pp.1-4.

[11] Fang Liu, Xiuzhen Cheng, and Dechang Chen, "Insider Attacker Detection in Wireless Sensor Networks," IEEE International Conf. on Computer Communications (INFOCOM), May 2007, pp. 1937-1945.

[12] David R. Raymond and Scott F. Midkiff, "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses," Pervasive computing, 2008, pp. 74-80.

[13] Issa Khalil, Saurabh Bagchi, Cristina N. Rotaru, Ness B. Shroff, "UnMask: Utilizing neighbor monitoring for attack mitigation in multihop wireless sensor networks," Ad Hoc Networks, in press, 2009.

[14] J. Lin, L. Xie, and W. Xiao, "Target tracking in wireless sensor networks using compressed KF," Int. J. Sensor Netw., vol. 6, nos. 3–4, Nov. 2009.

Jeena Elezabeth Cheriyan (M.E.Student, PSNACET, Dindigul) obtained her B.tech Degree in Computer Science and Engineering from Musaliar College of Engineering, Kerala in 2010 and currently pursuing M.E Degree in Computer Science in PSNACET, Dindigul. Her area of interests includes Wireless Sensor Networks, data warehousing/mining.

S. Sathees babu (Associate Professor, Depatment of CSE, PSNACET, Dindigul) received his B.Sc. Degree in Physics in 1996 through Vivekananda College, Sholoavandan, Madurai Kamaraj University and M.C.A. Degree in 1999 through the R.V.S. College of Engineering and Technology, Dindigul under Madurai Kamaraj University. He pursued his M.E. Degree in Computer Science and Engineering in 2006 from Anna University. He is pursuing his Doctorate Degree in Information and Communication Engineering from Anna University, Chennai. He has 15 years of teaching experience to UG and PG classes and has guided many B.E. and M.E projects. His research interests are Wireless Networks, Middleware Technologies and Distributed Computing. He has published 4 papers in International Journals and 15 papers in National and International conferences. He is a Life member of Indian Society for Technical Education.

K.Balasubadra(Professor and Head, Department of IT, RMD College, Chennai) received her B.E. Degree in Electronics and Communication Engineering in 1988 through PSNA College of Engineering and Technology, Dindigul Madurai Kamaraj University and M.E Degree in Applied Electronics through the Government College of Technology, Coimbatore under Bharathiar University in 1997. She received her Doctorate Degree in Information and Communication Engineering from Anna University, Chennai, in 2009. She has 23 years of teaching experience to UG and PG classes and has guided many B.E. and M.E projects. Currently, she is guiding 10 PhD scholars and also a research paper reviewer in conferences. She has published 5 research papers and 15 papers in international/national conferences. Her research interests are Analog VLSI, optical communications and wireless networks. She is a Life member of Indian Society for Technical Education and was a member in IEEE for more than 10 years. She is a recognized research supervisor of Anna University of Technology, Madurai.