ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)

On 21st&22nd March Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

Detection of Intruders in Wireless Sensor Networks Using Anomaly

A.Anbumozhi [1] , K.Muneeswaran[2]

[1]PG Scholar , Department Of Computer Science and Engineering, Mepco Schlenk Engineering College Sivakasi, India

[2] Professor, Department Of Computer Science and Engineering, Mepco Schlenk Engineering College Sivakasi, India

Abstract- Detecting Intruders in Wireless Sensor Networks plays an important role. Security in network aggregation is not an easy task. Sensor network consist of sensor nodes whose operation can be controlled by underlying network. In this paper, Sensors are used to sense the temperature, humidity, light, voltage etc in a particular area. Extended Kalman Filter (EKF) mechanism is proposed to filter the false data in sensor network. The false data can be acted by some event namely malicious, emergency event. Malicious event are acted by intruders, and Emergency event are acted by some accident occurrence eg. Fire. Intruders make the sensors to get the false reading therefore EKF mechanism is proposed. EKF monitors the behaviour of neighbours and predict their future states, each node aims at setting up normal range of the neighbor's future transmitted aggregated values. Using different aggregation functions (average, sum, max, and min), theoretical threshold value is calculated. Combining Cumulative Summation (CUSUM) and Generalized Likelihood Ratio (GLR) detection sensitivity can be increased. Intrusion Detection Modules (IDM) and System Monitoring Modules (SMM) work together in order to provide intrusion detection capabilities for WSNs. EKF address various uncertainties in WSNs and create an effective local detection mechanism.

Keywords – Cumulative summation(CUSUM),extended Kalman filter,generalized likelihood ratio (GLR),in-network aggregation,intrusion detection system, wireless sensor networks(WSNs).

I. INTRODUCTION

A **wireless sensor networks (WSNs)** typically consists of a collection of distributed sensor nodes which communicate with each other over a wireless medium. Sensors are used to sense the temperature, humidity, voltage etc at particular area. As soon as the sensor senses the information about a particular area they are propagated to base station. In turn, base station verifies the data sent by each sensor by comparing it with the predicted values. Therefore, malicious and emergency activities of a sensor are identified by base station.

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The modern networks are, bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by various military applications such as battlefield surveillance, boundary monitoring. Today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. A wireless network is any type of computer network that uses wireless data connections for connecting network nodes. The WSN is built of nodes from a few to several hundred or even thousands of nodes, where each node is connected to one (or sometimes several) sensors.

Each such sensor network node has typically several parts such as a radio transceiver with an internal antenna or an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form

of energy harvesting. Wireless telecommunications networks are generally implemented and administered using radio communication. This implementation takes place at the physicallevel (layer) of the OSI model network structure. Wireless sensor network (WSN) refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organize the collected data at a central location. Efficient delivery of sensed information could provide tremendous benefits to society. Wireless Sensor networks (WSNs) plays an important role to sense the coverage area and it provides effective and economically viable solutions for large variety of applications such as health monitoring, scientific data collection, environmental monitoring and military operation.

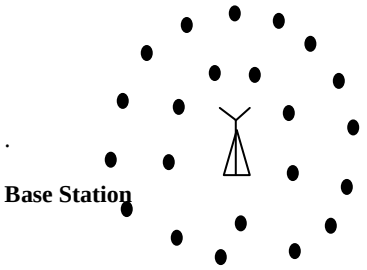


Fig 1.An example of wireless sensor nodes in a network sensing temperature in a particular area and reporting to base station.

Commonly monitored parameters are temperature, humidity, light, voltage etc. The ideal wireless sensor is networked and scalable,consumes very little power, is smart and software programmable,capable of fast data acquisition,reliable and accurate over the long term,costs little to purchase and install, and requires no real maintenance. Selecting the optimum sensors and wireless communication link requires the knowledge of the application and problem definition.Wireless Sensor Networks are composed of sensor nodes and sinks. Sensor nodes have the capability of self healing and self organizing. They are decentralized and distributed in nature where communication takes place via multi-hop intermediate nodes.The main objective of a sensor node is to collect information from its surrounding environment and transmit it to the sink.Anomaly-based IDS monitors network activities and classifies them as either normal or malicious using heuristic approach. Most of anomaly-based IDSs identify intrusions using threshold values i.e., that is, any activity below a threshold is normal, while any condition above a threshold is classified as an intrusion. The main advantage of anomaly-based IDS is its capability to detect new and unknown attacks. However sometimes it fails to detect even well-known security attacks.

Intrusion Detection System (IDS) is used for various detection mechanism such as to detect the intruders who violate the security policy in WSNs, to reduce the communication overhead, to detect and prevent immoral activities in WSNs, to achieve accurate detection result, to detect unusual behavior etc. To enhance security in wireless sensor network integration of System Monitoring Modules (SMM) and Intrusion Detection Module (IDM) work together. This integration can facilitate classification between malicious and important emergency events across the network..To filter it out, we go for Extended Kalman Filter (EKF) based mechanism.Combination of Cumulative Summation (CUSUM) and Generalized Likelihood Ratio (GLR) is performed to increase detection sensitivity.Sensor networks have started pursuing through every application in the real world, protecting the network has become a mandatory issue. Hence this paper proposes the detection of intruders in wireless sensor network..Detecting Intruders in sensors plays an important role. Nowadays, malicious event plays a vital role in network and submit a false report.Attackers explore vulnerabilitiesin a network and compromise sensor nodes as anomaly. The anomalies are further identified as events, and measured to detect across the wireless sensor network.

II RELATED WORK

Przydatek *et al.* [6] proposed an aggregate-commit-prove framework to design secure data aggregation protocols. Chan *et al.* [17] presented an optimally secure aggregation scheme for arbitrary aggregator topologies and multiple malicious nodes. Wagner [2] used statistical estimation to design more resilient aggregation schemes against malicious data injection attacks. In his work, a mathematical framework is presented to formally evaluate security of different aggregation algorithms.Bo Sunproposes Anomaly Detection Based Secure In Network Aggregation for Wireless Sensor Networks for detecting Intruders in wireless Sensor Networks. However, no detailed simulations and experiments are carried out in [2]. Moreover, [2] does not consider in-network aggregation. Our work improves over [2] in these aspects. Wu *et al.* [9] proposed a secure aggregation tree to detect and prevent cheating in WSNs, in which the detection of cheating is based on topological constraints in aconstructed aggregation tree.

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]–[16]. Also, a number of proposed protocols aim to ensure the secrecy and authentication of data [3]–[5] in WSNs. Several protocols are proposed to filter false data in WSNs[29]–[31]. Generally, they utilize different key distribution mechanisms to develop filtering capabilities. In these research 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. Kalman filter (KF) and CUSUM GLR have also been widely used in various applications. For example,in the context of WSNs, KF was used to enable accurate target tracking [40]. Based on nonparametric CUSUM, [41] proposed two local detector algorithms from sequential sensorreadings to enable distributed detection in WSNs. However,to the best of our knowledge KF and CUSUM have not yetbeen applied to secure WSN aggregation services.

III. MOTIVATION AND PROPOSED METHODOLOGY

Wireless sensor network (WSN) refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organize the collected data at a central location. Efficient delivery of sensed information could provide tremendous benefits to society. Wireless Sensor networks (WSNs) plays an important role to sense the coverage area and it provides effective and economically viable solutions for large variety of applications such as health monitoring, scientific data collection, environmental monitoring and military operation.

Sensor nodes are placed randomly in different places at different location to sense physical or environmental conditions, and hence the sensed values are reported to the base station. Sensing information about an particular area gives us as the importance. By detecting or by finding information we can predict the unusual happening across the network. eg if the temperature raises to an extend in an particular area then the base station raises an alarm which will be taken care by human operator.

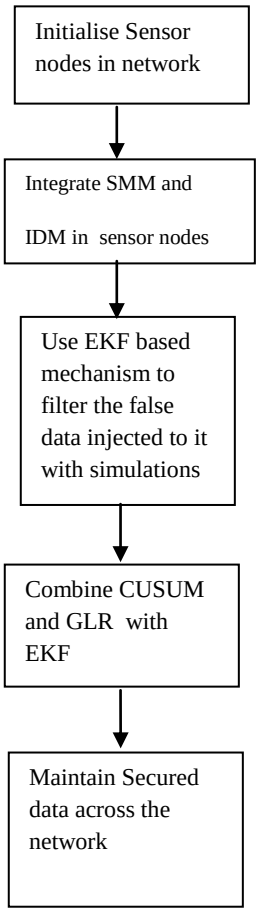


Fig 2 Steps in intrusion detection system

Once a sensor node is compromised, all its associated secrets become open to attackers, To solve this problem, intrusion detection systems (IDSs), which serve as the second wall of protection, can effectively help identify malicious activities. To enhance WSN security, we propose that system monitoring modules (SMM) should be integrated with intrusion detection modules (IDM) Malicious event plays a vital role in network and submit a false report. Attackers explore vulnerabilities in a network and compromise sensor nodes as anomaly. The anomalies are further identified as events,and measured to detect across the wireless sensor network . However, only a few protocols consider secure in-network aggregation based on a prevention-based scheme, in which encryption, authentication, and key management are usedin the context of WSNs. In practice, WSNs are often deployed to monitor important emergency events, such as forest fires and battlefield monitoring. This integration can facilitate classification between malicious events and important emergency events..IDM and SMM need to be integrated with each other to work effectively. Relying on local detection alone is not desirable because each node has only very limitedinformation available. Furthermore, since sensor nodes are prone to failure, it is very difficult to differentiate between emergency events sent by good nodes and malicious events.

In our proposed scheme, whenever IDM and SMM detect some abnormal events, they need to request the collaboration of more sensor nodes around the events to make a final decision. The intruders who violate the security policy in WSNsreduce the communication overhead.Security policy detect and prevent immoral activities in WSNs to achieve accurate detection results. Furthermore,since WSNs are usually densely deployed, nodes close to eachother can have spatially correlated observations, which canfacilitate the collaboration of sensor nodes in proximity to differentiatebetween malicious events and important emergencyevents. This motivates us to integrate SMM and IDM in orderto achieve accurate detection results. This motivatesour proposed local detection algorithms. Furthermore,since WSNs are usually densely deployed, nodes close to eachother can have spatially correlated observations, which canfacilitate the collaboration of sensor nodes in proximity to differentiatebetween malicious events and important emergencyevents.

The table1 illustrated below contains the notation used in Extended kalman filter and Cumulative Summation (CUSUM), Generalised Ratio (GLR). EKF can be applied to many nonlinear applications by approximating effects of small perturbations linearly.

TABLE 1
LIST OF SYMBOLS

SYMBOLS	MEANING
y_k	Noise
t_k	Actual value at time t_k
x_k	Initial State
z	Measured value at time t_k
H	Threshold value at time t_k
w_k	Process noise at time t_k
k_k	Kalman gain at time t_k

P_{01}	Temperature at time t_k
P_{02}	Variation of time t_k
S_n	Used to detect change in y_k
S_k	Simulation result of temperature
W	Window size
μ	Attack Intensity
Δ	Delta
K,n	Nodes

Each group of sensor nodes has a cluster head which report to base station act as sink. A, E, I, M sensor nodes act as cluster head for a group of nodes. Cluster head act as an intermediate node, each node aims at setting up a normal range of the neighbour's future predicted values. Each cluster has an aggregated value of sensed information by finding different aggregation functions (average, sum, max and min).The base stations are one or more components of the WSN with much more computational, energy and communication resources.They act as a gateway between sensor nodes and they typically forward data from the WSN on to a server. Other special components in routing based networks are routers, designed to compute, calculate and distribute the routing tables.An intrusion detection system (IDS) is a device that monitors network or system activities for malicious activities or policy violations and produces reports to a management station.

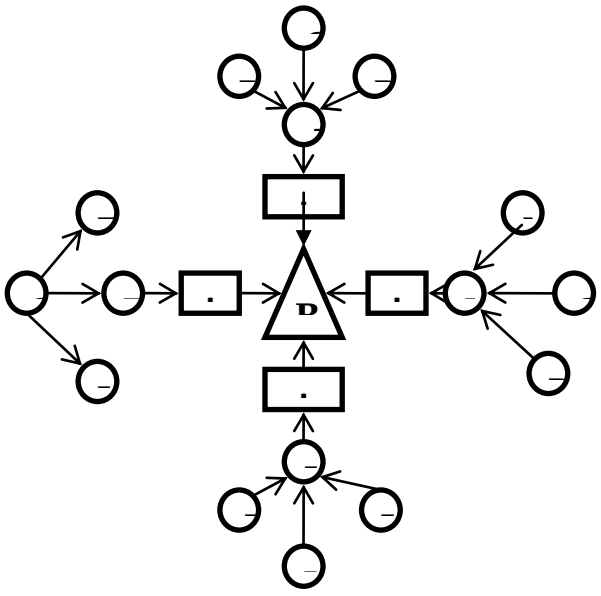


Fig.3.Architecture of Intrusion Detection System in Wireless Sensor Network

IV. SECURE IN NETWORK AGGREGATION

Network aggregation has been proven to be an important primitive to reduce the communication overhead and to save energy for WSNs. Many aggregation protocols have been proposed and their performance has been adjusted. However, only a few protocols consider secure in network aggregation based on a prevention-based scheme, in which encryption, authentication, and key management are used. Sensor networks have started pursuing through every application in the real world, protecting the network has become a mandatory issue. Hence this project proposes the detection of intruders in wireless sensor network. For the IDM, our general idea is like the mechanism proposed in [27]. Node A promiscuously overhears its neighbour's transmitted aggregated value and compares it with the predicted normal range. If the overheard value lies outside the normal range, either an event E happens or the neighbour N then becomes a suspect. To tell whether node N is a malicious node or E is an important emergency event like the breakout of a forest fire, A initiates the collaboration between IDM and SMM by waking up relevant sensor nodes around N and requesting their opinions about E. Please note that our proposed detection solution and the solution adopted in [27] are completely different.

V. IMPLEMENTATION AND RESULTS

Implementation methodology of the proposed system explains how the malicious and emergency activities are detected in a sensor network. 54 sensors are placed in 54 labs to sense the particular area. This dataset contains information about data's collected from 54 sensors which were deployed in the Intel Berkeley Research lab dated between February28th to April5th, 2004. Sensor reading consists of date, time, epoch value, mote-id, temperature, humidity, light, voltage.This dataset includes a log of about 2.3 million readings collected from sensors.

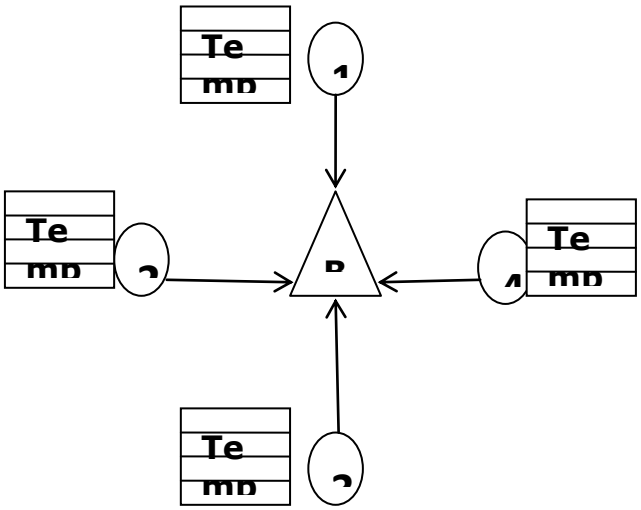


Fig.4. An examplein which each sensor has the sensed information,reporting to base station

Implementation has the following steps to follow

A)Analyze Dataset :

For example, we can use Intel Lab Data[33], a commonly used data set, to plot the relationship *F* between $x_k$and x_{k+1} in an environment similar to the Intel

Berkeley Research Laboratory. We randomly pick one sensor node, filter out its faulty readings (i.e., those readings that deviate much from both immediately previous and following readings), and select one time period in which temperature readings keep increasing. Basedon the readings in this time period, we plot the relationship between $x_k$and x_{k+1}This dataset contains information about data's collected from 54 sensors which were deployed in the Intel Berkeley Research lab dated between February 28th to April 5th, 2004. Sensor reading consists of date, time, epoch value, moteid, temperature, humidity, light, voltage.This dataset includes a log of about 2.3 million readings collected from sensors.In this case, Epoch is a monotonically increasing sequence number from each mote,Two readings from the same epoch number wereproduced from different motes at the same time.Temperature is in degrees Celsius, Humidity is temperature corrected relative humidity, ranging from 0-100%.Light is in Lux, Voltage is expressed in volts, ranging from 2-3.

B)Extended Kalman Filter:

EKF finds the false data injected to the dataset .It identifies the data and differentiates them into emergency and malicious event.Implementation works with false data injected to base station.Sensor node monitors its neighbor's behavior and predicts a normal range of the neighbor's future aggregated values.Creation of normal range is calculated with estimated values by EKF.

EKF can be applied to many nonlinear applications by approximating effects of small perturbations linearly. By setting a proper process model and measurement model for a specific WSN application and utilizing time update and measurement update equations to recursively process data, we can use EKF to obtain a relatively accurate estimate of state [25].

Example
Data injected to the dataset
Sensor node no : 36
Emergency alert : FIRE
Enter alert temperature : 27.8

Base station check the input with dataset
36
FIRE
27.8

Algorithm 1EKF based local detection algorithm

Input: Node n_i, Temperature $temp_i$
Output: alert Fire, alert Intruder
Establish WSN ( )
init Parameter ( )
for each node n_i
{
$temp_i$ = read temp(n_i);
flag = isEmergent($temp_i$);
if(flag)
{
valid = checkValidity( );
if(valid)
alert Fire( )
else
alert Intruder(i)
}
}

Moreover,emergency temperature given by node is checked with actual temperature in dataset.If the temperature violates in neigbour nodes then the base station alerts the whole process.If the majority of nodes reply that event E could happen,then Sensor node makes a decision that E is triggered by some emergency event.On the other side, if the majority of nodes reply that E could not happen, then A makes a decision that E is triggered by some malicious event.

EKF can be applied to many nonlinear applications by approximating effects of small perturbations linearly. In our case, 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. Furthermore, individual sensor readings are subject to environmental noise. To demonstrate this, we set up a simple one-hop WSN testbed, in which node A periodically transmits sensed values to a base station. Node A consists of a MICA2 mote and a MTS310 sensor board [24].

Sensor nodes suffer from stringent resources, which prevent the usage of some powerful yet expensive estimation and prediction approaches. To enable neighbour monitoring mechanisms, we need a lightweight scheme that can be efficiently executed by sensor nodes. In this respect, we use an approach based on EKF for each node to predict and estimate future values of its neighbours. The following example gives the malicious event, emergency event for detecting the intruders in wireless sensor networks.We conduct experiments and simulations to evaluate EKF based and CUSUM GLR based local detection mechanisms using different aggregation functions. Our implementation ofEKF and CUSUM GLR on representative sensor node MICA2motes [23] demonstrates that our proposed scheme is practicalon resource stringent hardware.

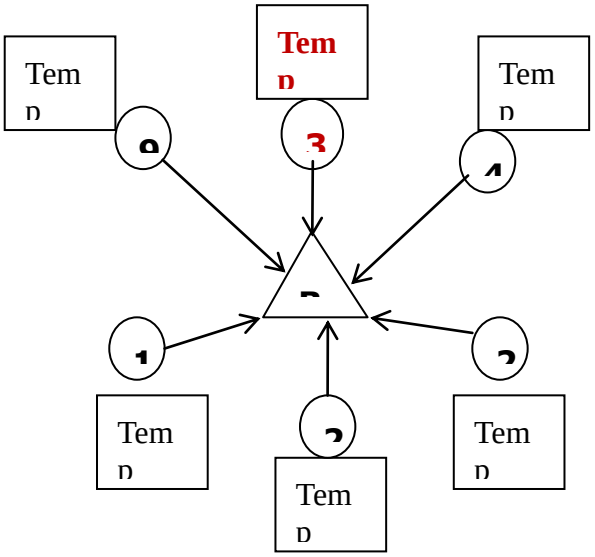


Fig.5.Extended Kalman Filter based local detection for Malicious Event

As the temperature is not overheared by other neighbour nodes. There is no such emergency event happened. It works normally. Therefore node : 36 is said to be an Malicious actor as the neigbour nodes reply that E(fire) could not happen , it is said to be malicious event, relatively accurate prediction of neighbours future aggregated values.

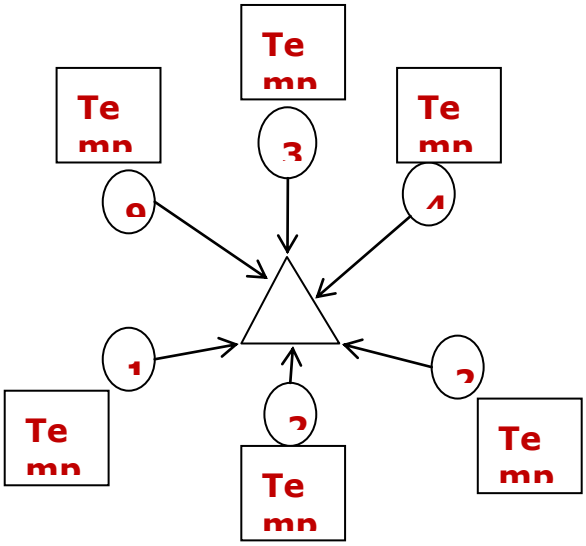


Fig.6. Extended Kalman Filter based local detection for Emergency event

As the temperature is overheared by other neigbour node. Fire event had happened. Therefore, base station raises an alert to overall sensor nodes.

C)Threshold Based Anomaly Detection Mechanisms:

Now, we present our EKF based local detection algorithm. Asensor node monitors its neighbour'sbehaviour and establishesa normal range of the neighbour's future aggregated values.The creation of the normal range is centred on estimated values using EKF. An alert can be raised if the monitoredvalue lies outside of the predicted normal range. This schemeis illustrated in Algorithm 1finds a predefined threshold.

D) CUSUM GLR Based Local Detection:

An EKF based approach does notconsider the fact that attacks launched at different times are not always independent. Therefore, an EKF based approach ignores the information given by the entire sequence of measured values. For example, in Algorithm 1, if an attacker continuously forges *zk*+1 with small deviations, this leads to a small Diff. A relatively largecan make an EKF based approachinsensitive to these kinds of attacks because this approaches only.In order to increase the detection, CUSUM and GLR algorithm is applied. As the false data is identified by EKF the particular node data are taken into consideration for this module. Due to resource constraints on sensor nodes, it is difficult for sensor nodes to carry out complex operations. Also, it consumes much memory to store in sensor nodes. Therefore, necessary simplifications are needed. This CUSUM and GLR have the following process calculated for particular intruder node. As EKF, threshold value is calculated termed as attack intensity. Based on attack intensity CUSUM, GLR decides the alert generation. When injected falsified values have small deviations, an EKF based approach alone may not achieve desirable performance. Therefore, in this section, based on EKF, we further apply analgorithm of combining CUSUM and GLR [1], which utilizesthe cumulative sum of the deviations between measured valuesand estimated values.

1) Basic Principles of CUSUM GLR:

Each sensor nodes are surrounded by neighbours, each node aims at setting up a normal range of future transmitted aggregated values. As each sensor node has different sensed value. Detecting intruder is not an easy task. Depending upon the neighbour temperature value the following measurement is done. To form decision rules to detect the change, weapply CUSUM GLR because it has illustrated overall desirable performance [32]. We first define the log-likelihood ratio as

$$S_k=\log_2 (p_{o1}/p_{o2});$$

Intuitively, $s_k$shifts from a negative value to a positive one when a change occurs in parameter. We further define

$$S_n = \text{Summation } (S_k);$$

2) *Combination of Extended Kalman Filtering andCUSUM GLR:*

EKF estimate errors when there is no anomaly happening. For particular identified temperature attack density is calculated and alarm is raised. S_n value is compared with threshold value named attack intensity.

Where,

μ -Attack Intensity,

W - Window Size

μ -1/w $\sum y_k$

y_k– Dataset temperature-Current Input temperature.

The length of time that it can take to generate alarms depends on attack density. The more intense the attack is,

the more quickly S_N can reach the predefined threshold h to generate alarms.

Decision Rule

```
{
   d='H0' if Sn<h
   d='H1' if Sn>=h
}
```

Detect Anomaly

d=H0 is a string which raises an alert to the neigbour node, It is considered to be emergency. Emergency for event identified get Alarm, where d=H1 raises no alert to the system, it performs normally.The length of time that it can take to generate alarmsdepends on attack intensity. The more intense the attack is, the more quickly $S_n$can reach thepredefined threshold hto generate alarms.

3) *CUSUM GLR Based Anomaly Detection:*

Due to resourceconstraints on sensor nodes, it is difficult for sensornodes to carry out complex operations such as *ln* in (9). Also, it consumes much memoryto store in sensor nodes. Therefore, necessarysimplifications are needed. We assume that the standard variation of $y_k$before the anomaly, and the standard variation of after the anomaly,This task is challenging because of potential high packet loss rate [18], harsh environment, sensing inaccuracy,time asynchrony between children and parents' nodes, and so on.

Algorithm 2CUSUM GLR Based local detection

Step 1: Get measured estimate value from Extended kalman filter.Assign the variation of values in H0 && H1.
Step 2: Measure N, S_n. where S_n = summation(S_k) where k=0=N,S_k = ln(p01/po2);
Step 3: Combination of EKF and CUSUM GLR
Step 4: Assign the window Size and threshold values.
If S_n< threshold value, Then d="H0";
else if S_n>= threshold value
d="H1";

---

filter CUSUM( ),GLR( )
Input : Temp $temp_i$, threshold h, node n_i, EKF( )
Output : alertAlarm( ), alertIntruder( )
Establish EKF( )
initParameter( )
for each node n_i

```
{
    N      = tempi;
    tempi  = Sn;
    Sn     = ∑(Sk);
    Sk     = log2(po1/p02);
}
```

---

4)Collaboration Between IDM and SMM : Local detection alone is not enough. WSNs are oftendeployed to monitor emergency phenomena (like the breakout of a forest fire), about which good nodes can trigger important events and generate unusual yet important information. Also, the error prone nature of sensor nodes may make even normal sensor nodes faulty and generate abnormal information. Therefore, local detection alone suffers from a high false positiverate. Node collaboration is necessary for sensor networks to make correct decisions about abnormal events. Therefore, for WSNs, IDM and SMM need to integrate with each other to work effectively. When node Araises an alert on node *B* because of some event E, to decide whether Eis malicious or emergent, *A* may initiate a further investigation on E by collaborating with existing SMMs. WSNs are usually densely deployed to collaboratively monitor some events. Based on this, node Acan wake up those sensor nodes (denoted as co detectors around Band request from these nodes their opinions on the behaviour of E. Becausethe majority of sensor nodes around the investigated event Eare not compromised, after Acollects the information fromthese nodes, if Afinds that the majority of sensor nodes think that event Emay happen, Athen makes a decision that Eis triggered by some emergency events. On the other hand, if Afinds that the majority of sensor nodes think that event Eshould not happen, Athen thinks that *E* is triggered by either a malicious node or a faulty yet good node. In this way, Acan continue to wake up those nodes around event Eand their opinions about the behaviour of E. If Akeeps finding that the majority of sensor nodes think that event Eshould not happen, Athen suspects that *E* is malicious. After Amakes a final decision, Acan report this event to base stations. No matter whether it is an emergency event or a malicious event, the event can be taken care of by human operators. These results are identified where

- IDM monitors malicious event.
- SMM monitors emergency event.
- Also, the error prone nature of sensor nodes may make even normal sensor nodes faulty and generate abnormal information. Therefore, local detection alone suffers from a high false positive rate.

- Node collaboration is necessary for sensor networks to make correct decisions about abnormal events.
- WSNs are usually densely deployed to collaboratively monitor some events.
- To save energy, some sensor nodes are periodically scheduled to sleep.

VI. PERFORMANCE EVALUATION

In this section, we use live data and synthetic data to evaluate EKF based and CUSUM GLR based location detection algorithms. The advantage of live data is that they capture real-world situations. However, live data only contain a limited number of situations whoseparameters cannot be varied. The following two metrics is used to evaluate EKF based algorithm.

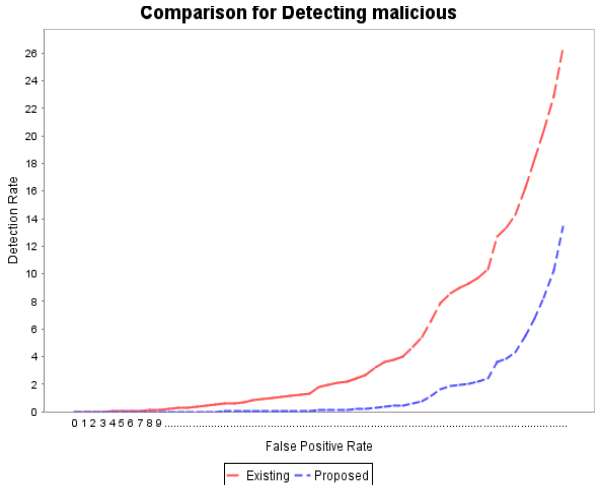
1) False positive rate: It is measured over normal data items. Suppose that mnormal data items are measured, and nof them are identified as abnormal. False positive rate is defined as n/m.

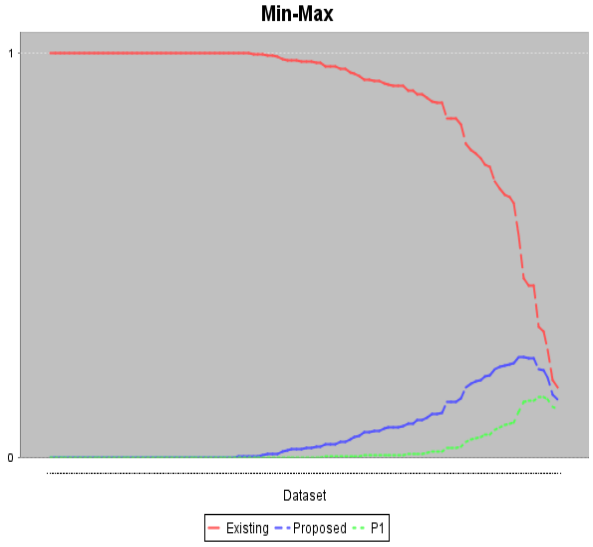
2) Detection rate: It is measured over abnormal data items. Suppose that *m* abnormal data items are measured,

and *n* of them are detected. Detection rate is defined as n/m.

When we evaluate the EKF based detection scheme, in the case of the same distribution of vi, we make all $v_i$randomlydistributed between one predefined range [min, max]. In thecase of the different distribution of v*i*, we set different *vi* randomly distributed between different [min, max].pairs. Since the simulation results of average, sum, maximum, and minimumare similar, we only illustrate the simulation of theaverage aggregation.

We have similar simulation results and observationsbetween the average aggregation and other aggregation functions, such as sum, min, and max. Therefore, we only present the results of the average function in the following.For the same distribution of $v_i$under normal operations, thechange of $S_N$and $S_k$for average aggregations under differentpacket loss rates is plotted.The following graph shows the evaluation of detecting malicious and the aggregation values of min-max.Unlike existing techniques, our work aims at addressing secure in-network aggregation problems from an intrusion detection perspective. Our work relies on predicted aggregated values in an efficient online manner and can complement existing aggregation protocols to considerably enhance WSN security. To increase detection sensitivity when malicious valueshave smalldeviations, we further apply an algorithm ofcombining cumulative summation (CUSUM) and generalizedlikelihood ratio (GLR) [1].





VII.CONCLUSION AND FUTURE WORK

IDM and SMM should work together to provide intrusion detection capabilities for WSNs.IDM detect malicious event.SMM detect emergency event.EKF based approach is proposed to detect false injected data and used to address various uncertainties in WSNs and therefore creates an effective local detection mechanism.Moreover to increase detection sensitivity, an algorithm of combining CUSUM and GLR is proposed**.**

In the future work, the objective function can be made more robust and effective. This includes considering more parameters in the EKF and CUSUM GLR based local detection.

ACKNOWLEDGEMENT

The authors wish to express their sincere thanks to the department of computer science and engineering of Mepco Schlenk College, Sivakasi for providing valuable guidelines,good support and encouragement during this work.They are also thankful to the management and principal for their constant support and encouragement to carry out this part of the project work successfully.

REFERENCES

[1]J.-Y. Chen, G. Pandurangan, and D. Xu, “Robust computation of aggregates in wireless sensor networks: Distributed randomized algorithms and analysis,” IEEE Trans. Parallel Distributed Sys., vol. 17, no. 9, pp. 987–1000, Sep. 2006.

[2]A. Manjhi, S. Nath, and P. B. Gibbons, “Tributaries and deltas: Efficient and robust aggregation in sensor network streams,” in Proc. ACMSIGMOD, 2005, pp. 287–298.

[3]S. Roy, S. Setia, and S. Jajodia, “Attack resilient hierarchical data aggregation in sensor networks,” in *Proc. ACM SASN*, 2006, pp. 71– 82.

[4]H. Chan, A. Perrig, and D. Song, “Secure hierarchical InNetwork aggregation in sensor networks,” in Proc. ACM CCS, 2006, pp. 278–287.

[5]J.Zhao and R. Govindan, "Understanding packet delivery performancein dense wireless sensor networks," in Proc. ACM Sensys, Nov. 2003,pp. 1–13.
[6]R. Pon, M. Batalin, M. Rahimi, Y. Yu, D. Estrin, G. J. Pottie, M.Srivastava, G. Sukhatme, and W. J. Kaiser, "Self-aware distributedembedded systems," in Proc. IEEE FTDCS, May 2004, pp. 102–107.
[7]D. Chu, A. Deshpande, J. M. Hellerstein, and W. Hong, "Approximatedata collection in sensor networks using probabilistic models," in Proc.IEEE ICDE, Apr. 2006, pp. 48–59.
[8]M. C. Vuran et al., "Spatial-temporal correlation: Theory and applicationsfor wireless sensor networks," Elsevier Comput. Netw., vol. 45, no.3, pp. 245–259, Jun. 2004.
[9]G. Wang, W. Zhang, G. Cao, and T. La Porta, "On supporting distributedcollaboration in sensor networks," in Proc. IEEE Milcom, vol. 2. Oct.2003, pp. 752–757.
[10]*Mica2 Mote* [Online].Available: http://www.memsic.com.
[11]M.S.Grewal and A. P. Andrews, Kalman Filtering: Theory and PracticeUsing MATLAB. New York: Wiley, Jan. 2001.
[12]D. C. Montgomery, Introduction to Statistical Quality Control. NewYork: Wiley, 2009.
[13]S.Marti, T.J. Giuli, K. Lai, and M. Baker, "Mitigating routingmisbehaviour in mobile ad hoc networks," in Proc. ACM Mobicom, Aug.2000, pp. 255–265.
[14]D.J.Abadi, S. Madden, and W. Lindner, "REED: Robust, efficientfiltering and event detection in sensor networks," in Proc. VLDB, 2005,pp. 769–780.
[15]Z. Yu and Y. Guan, "A dynamic en-route scheme for filtering false datainjection in wireless sensor networks," in Proc. IEEE INFOCOM, Apr.2006, pp. 1–12.
[16]F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route detectionand filtering of injected false data in sensor networks," in Proc. IEEEINFOCOM, Mar. 2004, pp. 2446–2457.