International Journal of Research In Science & Engineering e-ISSN: 2394-8299
Volume: 3 Issue: 4 July-August 2017 p-ISSN: 2394-8280

TRUST AND ITERATIVE FILTERING APPROACHES FOR SECURE DATA COLLECTION IN WIRELESS SENSOR NETWORKS

Dr. Shoban Babu[1],Prof. Mangesh Ingle[2],Prof. Ashish Mahalle[3]
Designation: Associate Professor , Department of Computer Engineering,
Varadha Reddy College of Engineering, SR Group of Colleges
[2,3]JCOET, Yavatmal

babuack@yahoo.com

As the computational power of very low power processors dramatically increases, mostly driven by demands of mobile computing, and as the cost of such technology drops, WSNs will be able to afford hardware which can implement more sophisticated data aggregation and trust assessment algorithms. Iterative Filtering (IF) algorithms are an attractive option for WSNs because they solve both problems data aggregation and data trustworthiness assessment using a single iterative procedure. The algorithm simultaneously aggregate data from multiple sources and provide trust assessment of these sources, usually in a form of corresponding weight factors assigned to data provided by each source. The current IF algorithms are vulnerable at collusion attack strategy. We propose a solution for such vulnerabilities by providing an initial trust estimate which is based on a robust estimation of errors of individual sensors. When the nature of errors is stochastic, such errors essentially represent an approximation of the error parameters of sensor nodes in WSN such as bias and variance. However, such estimates also prove to be robust in cases when the error is not stochastic but due to coordinated malicious activities. Such initial estimation makes IF algorithms robust against described sophisticated collusion attack, and, we believe, also more robust under significantly more general circumstances. We built a prototype application to simulate and demonstrate the proof of concept.

Index Terms – WSN, secure data aggregation, compromising nodes, IF algorithms

INTRODUCTION

Due to a need for robustness of monitoring and low cost of the nodes, wireless sensor networks (WSNs) are usually redundant. Data from multiple sensors is aggregated at an aggregator node which then forwards to the base station only the aggregate values. At present, due to limitations of the computing power and energy resource of sensor nodes, data is aggregated by extremely simple algorithms such as averaging. However, such aggregation is known to be very vulnerable to faults, and more importantly, malicious attacks. For that reason data aggregation at the aggregator node has to be accompanied by an assessment of trustworthiness of data from individual sensor nodes. Trust and reputation have been recently suggested as an effective security mechanism for Wireless Sensor Networks. Sample WSN is presented in Figure 1.

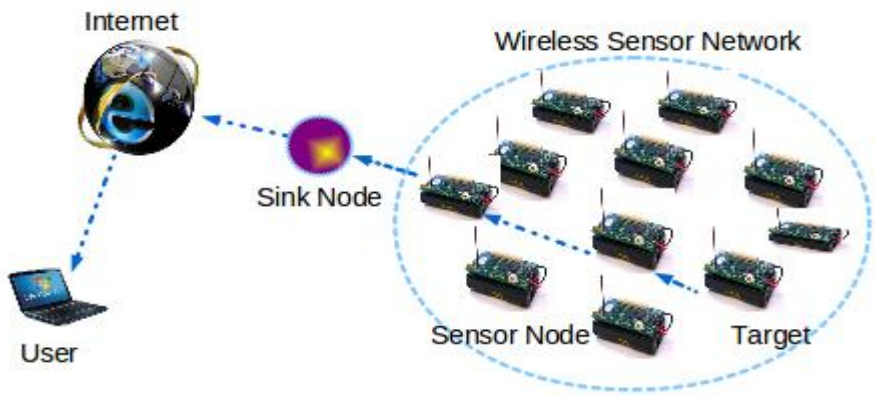


Figure 1 – Sample WSN

As shown in Figure 1, it is evident that there are many sensor nodes meant for sensing data and they can send the sensed data to sink node. Through Internet users can access such data hen WSN is connected to Internet using a gateway. In this scenario it is very important to have data aggregation in order to have efficiency in data gathering and dissemination. Therefore secure data aggregation became an inevitable choice. Many researchers contributed towards it. Iterative filtering algorithms, compromised node detection and trust and reputation based approaches are the three areas in which literature is available. Iterative Filtering (IF) algorithms are an attractive option for WSNs because they solve both problems data aggregation and data trustworthiness assessment using a single iterative procedure. The algorithm simultaneously aggregate data from multiple sources and provide trust assessment of these sources, usually in a form of corresponding weight factors assigned to data provided by each source. The current IF algorithms are vulnerable at collusion attack strategy. Our ContributionIn this paper we proposed an algorithm hat can overcome the issues with existing IF schemes. The proposed algorithm ensures secure data aggregation in presence of a potential adversary who targets the WSN for injecting false aggregation values. We built a prototype application to demonstrate the proof of concept.The remainder of the paper is structured as follows. Section II provides review of literature. Section III presents the proposed system in detail. Section IV presents experimental results while section V concludes the paper.

RELATED WORKS

This section provides review of literature on secure data aggregation in WSNs. Many researchers contributed towards providing secure data aggregation schemes for robust communications in WSN. Iterative filtering algorithms, compromised node detection and trust and reputation based approaches are the three areas in which literature is available. As many as six algorithms were proposed by Li et al. in [2]. All approaches are iterative in nature and they looked similar. Norm and aggregation functions differed among all three algorithms. Later on Ayday et al. [3] proposed IF algorithm which was slightly different. The differences from other IF algorithms are as follows. There is time-discount factor that causes the rating to fade out over a period of time. Black list of users is maintained by the algorithm for bad raters. Liao et al. in [4] proposed an algorithm that is iterative in nature but also uses social network of users besides rating matrix. Bias smoothed tensor model was introduced by Chen et al. [5] which is based on Bayesian model which is very complex in nature. Simple cheating behaviour is expected from adversaries by IF algorithms. However, IF did not take into account the collusion attacks and malicious scenarios. In this paper we considered trust and reputation in our enhanced IF algorithm. A general reputation framework was proposed by Generiwal et al. [7] where each node involves in estimating reputation of other nodes by observing neighbours. In the same fashion, Xiao et al. in [8] proposed trust based approaches in order to correlate faulty data dissemination. They also proposed a ranking mechanism for leveraging trust in order to ensure that sensor nodes behave well. PRESTO is architecture proposed by Li et al. [9] for hierarchical sensor network. It is a two – tier framework that makes use of proxy nodes for storing sensed data. Between data items and network nodes, Lim et al. in [1] proposed an interdependency relationship for finding trust associated with the nodes in the network. A combination of trust, fault tolerance, and data aggregation were proposed by Sun et al. [10] for WSNs that involve in multimedia communications. A trust based framework was proposed by Tang et al. [11] for special WSN such as battle-network where it is very important to protect nodes from enemies with a command and control centre in place. Trust and reputation models are widely used to handle fault detection issues in WSN. However, they did not take into account collusion attacks in hostile environments where WSN is deployed. In fact trust and reputation models can be used to overcome problems such as compromised nodes that are involved in data aggregation.
In order to find out compromised nodes in WSN, Ho et al. in [12] proposed a framework that makes use of software attestation. The revocation of compromised nodes is also explored by them as they provide highly risky environment with false positives in the proposed scheme. False aggregator detection and its importance was explored in [13] by making use of a MAC value along with aggregation results. However it was observed that high remission cost and high computation cost are required to ensure MAC based integrity thus the scheme may not be suitable for most of the networks.

e-ISSN: 2394-8299
p-ISSN: 2394-8280

A defence strategy based on game-theory was prepared by Lim et al. [6] in order to safeguard interests of nodes in WSN with the guarantee of trust for the data that has been sensed. These studied revealed many interesting facts. For instance they found that false aggregation operations are carried out by adversaries on the nodes that are involved in data aggregation. This was to obtain the data and inject false aggregate values in order to achieve malicious objectives of adversaries. The result of such attacks is that false data is provided to concerned authority and the decisions take on such data are not accurate. When nodes are compromised, they are to be handled effectively and there is no potential risk when compromised nodes are identified and removed from network. False data injection has been around and that is considered to conduct the research in the given scenario with existing knowledge and expected collusion attacks by compromising nodes with technical knowhow and the algorithms defined.

PROPOSED AGGREGATION SCHEME

As shown in Figure 2, it is evident that there are different parties involved in the scheme. They include service provider, router, attacker model, sensor nodes, and base station. Sensor nodes sense data pertaining to temperature and send it to base station. However, some other node might act as router in order to send the data to base station. The basis scenario is presented that shows how the purpose of the nodes in WSN is served. There are aggregator nodes that take care of data aggregation before sending data to base station. Now the problem is to effectively protect aggregator nodes and WSN for that matter from malicious attacks including collusion attacks.

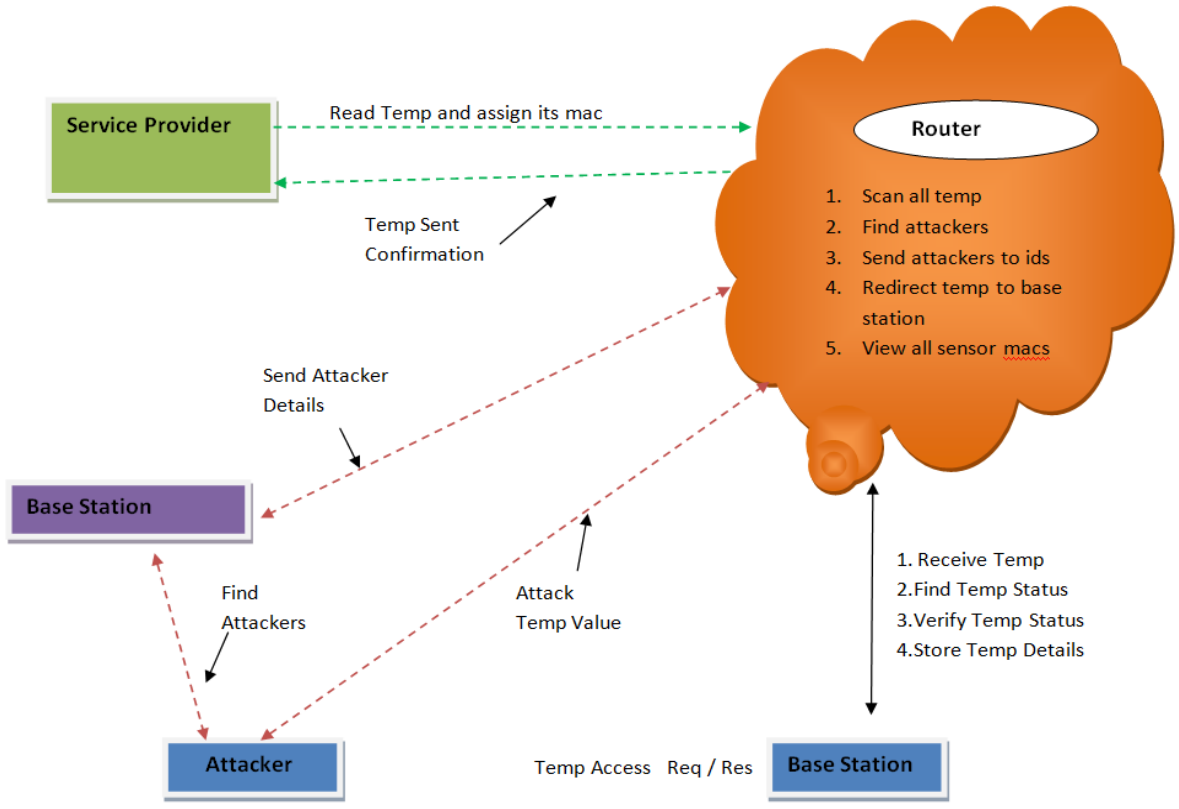


Figure 2 – Architectural overview of the proposed system

Attacker is assumed to have information about the sensor network and willing to make attacks. Attacker generally injects faulty values in to the network so as to discourage decision making process. The base station is able to receive sensed data and maintain the data. When attacks are made it is

e-ISSN: 2394-8299
p-ISSN: 2394-8280

important to protect the WSN from malicious activities. More details on the parties involved including their actions are presented in Figure 3.

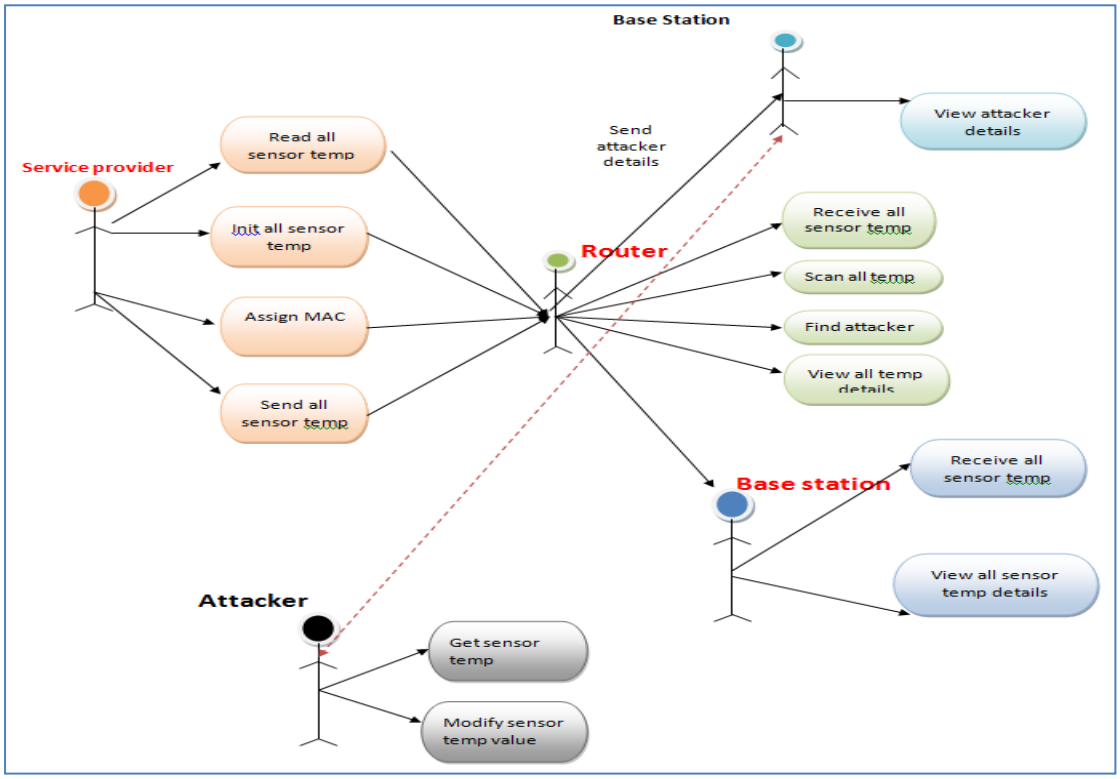


Figure 2 – Interaction among different players involved in the system

The service provider is able to read sensor temperatures, assign MAC and send all details. The router sends attack details to base station. The router receives data, scans it, fins attack probabilities and take necessary steps. The base station is able to reveal temperature data and view the same. The base station also can view attack details if found. The following is the algorithm employed in order to achieve enhanced IF.

Algorithm: Enhanced Iterative Filtering Algorithm
Inputs: Data from multiple sources
Outputs: Secure data aggregation

Initialization
01 Initialize nodes ***N***
02 Initialize vectors to hold data ***V***
03 Initialize ***suspect*** to false
04 Initialize suspected nodes ***SN***
05 Initialize a model M
Enhanced Iterative Filtering
06 While true Do
07 For Each n in N
08 For Each v in V
09 Build/update model M
10 IF v has abnormality THEN
11 suspect=true

```
12              Add n to SN
13          End For
14      End For
15      Avoid suspected nodes
16      Aggregate only data from genuine nodes
17  END IF
```

Algorithm 1 – Enhanced Iterative Filtering Algorithm

As shown the algorithm takes data from multiple sources and performs secure data aggregation. It has initialization and enhanced iterative filtering phases. It makes use of vectors to hold data and performs iterative filtering to know abnormalities. It avoids suspected nodes and aggregates only the data from genuine nodes.

IMPLEMENTATION AND RESULTS

Implementation is done using Java programming language. It has many models as described below. It makes use of the proposed algorithm to simulate and demonstrate the proof of concept.

Service Provider

In this module, the Service Provider activates all the sensors and assigns temperatures to the sensor node, and backup temperature will be stored, uploads their data to the particular base station. It will store in node. The service provider, can view the attacked file by the Base Station, He can replace the injected fake temperature to the sensor node.

Router

In this module, the predicate count query is used to determine the total number of nodes whose sensor readings have some property in the network. And it is responsible for delivering the sensor readings to the Base stations. If he founds fake temperature readings then it transfer the flow to Base Station. Before sending any file to receiver temperature will be verified, then send to particular base station. In a router we can view the sensor temperature details and clear the details.

Base Station

In this module, The base station collecting all sensor nodes (sn1, sn2, sn3, sn4, sn5….) and computing aggregation results at the base station (BS), in network aggregation allows sensor readings to be aggregated by intermediate nodes, which efficiently reduces the communication overhead. The Base Station used for checking the temperature status and to verifies the results through reliable random sampling achieved by data commitment and interactive proofs with the base station.

Attacker

Attacker is one who is injecting the fake temperature to the particular sensor node. And Router will identify the attackers, then stored in attacker list.

e-ISSN: 2394-8299
p-ISSN: 2394-8280

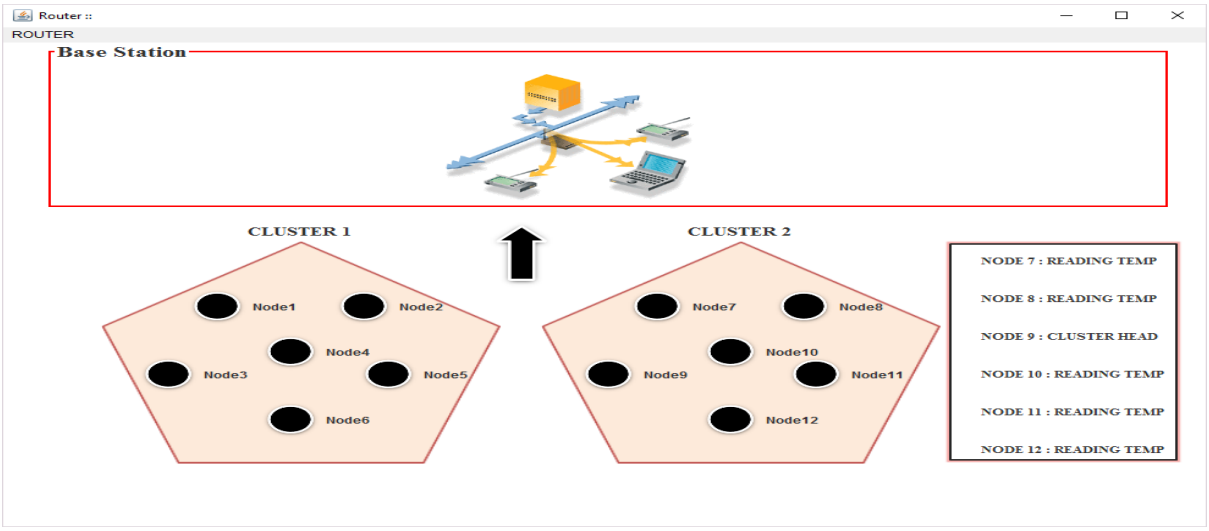
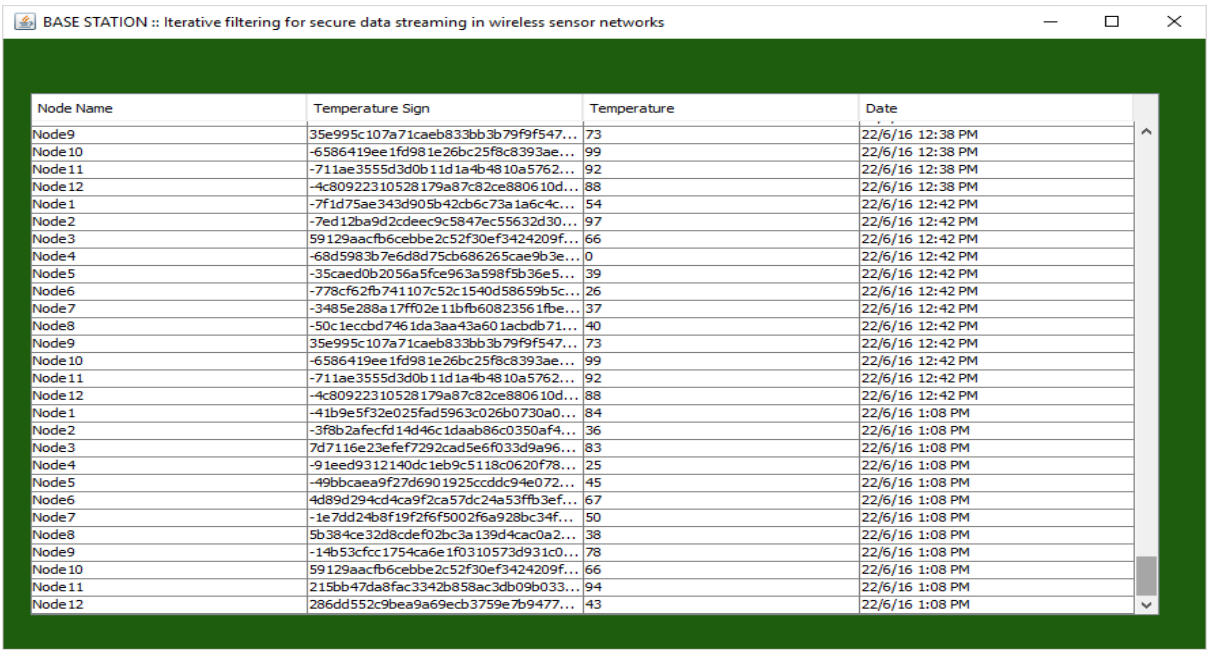


Figure 4 – Shows simulation scenario

As shown in Figure 4, there are clusters of nodes and node status is being presented. The nodes perform as per their purpose and the data is sent to base station. In the process the proposed algorithm is employed in order to detect any malicious activities. The secure data aggregation of data from different nodes is presented in Figure 5.

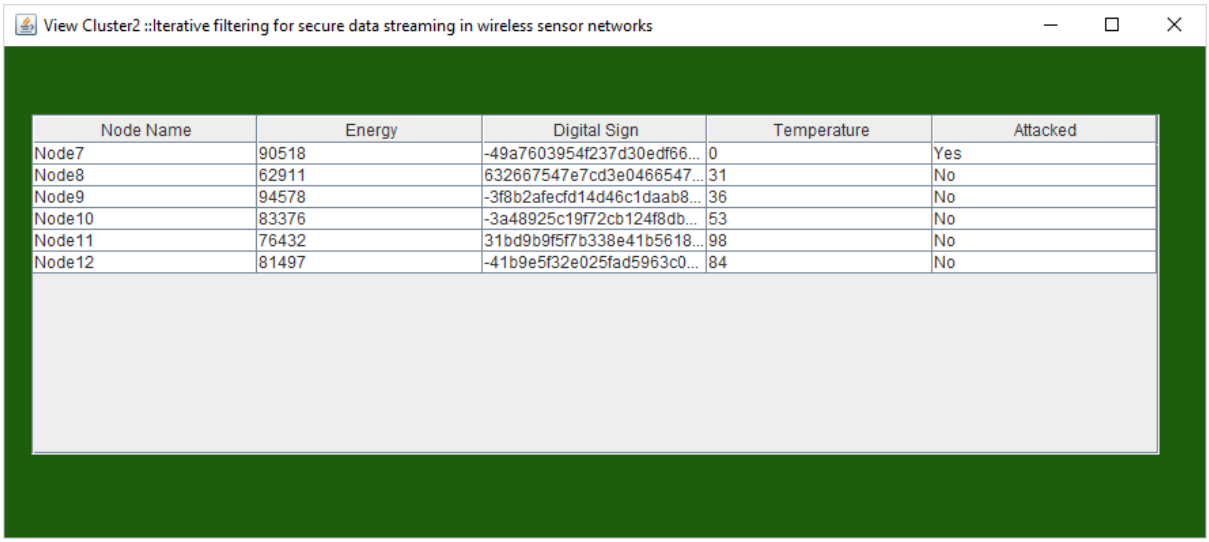


Node Name	Temperature Sign	Temperature	Date
Node9	35e995c107a71caeb833bb3b79f9f547...	73	22/6/16 12:38 PM
Node10	-6586419ee1fd981e26bc25f8c8393ae...	99	22/6/16 12:38 PM
Node11	-711ae3555d3d0b11d1a4b4810a5762...	92	22/6/16 12:38 PM
Node12	-4c80922310528179a87c82ce880610d...	88	22/6/16 12:38 PM
Node1	-7f1d75ae343d905b42cb6c73a1a6c4c...	54	22/6/16 12:42 PM
Node2	-7ed12ba9d2cdeec9c5847ec55632d30...	97	22/6/16 12:42 PM
Node3	59129aacfb6cebbe2c52f30ef3424209f...	66	22/6/16 12:42 PM
Node4	-68d5983b7e6d8d75cb686265cae9b3e...	0	22/6/16 12:42 PM
Node5	-35caed0b2056a5fce963a598f5b36e5...	39	22/6/16 12:42 PM
Node6	-778cf62fb741107c52c1540d58659b5c...	26	22/6/16 12:42 PM
Node7	-3485e288a17ff02e11bfb60823561fbe...	37	22/6/16 12:42 PM
Node8	-50c1eccbd7461da3aa43a601acbdb71...	40	22/6/16 12:42 PM
Node9	35e995c107a71caeb833bb3b79f9f547...	73	22/6/16 12:42 PM
Node10	-6586419ee1fd981e26bc25f8c8393ae...	99	22/6/16 12:42 PM
Node11	-711ae3555d3d0b11d1a4b4810a5762...	92	22/6/16 12:42 PM
Node12	-4c80922310528179a87c82ce880610d...	88	22/6/16 12:42 PM
Node1	-41b9e5f32e025fad5963c026b0730a0...	84	22/6/16 1:08 PM
Node2	-3f8b2afecfd14d46c1daab86c0350af4...	36	22/6/16 1:08 PM
Node3	7d7116e23efef7292cad5e6f033d9a96...	83	22/6/16 1:08 PM
Node4	-91eed9312140dc1eb9c5118c0620f78...	25	22/6/16 1:08 PM
Node5	-49bbcaea9f27d6901925ccddc94e072...	45	22/6/16 1:08 PM
Node6	4d89d294cd4ca9f2ca57dc24a53ffb3ef...	67	22/6/16 1:08 PM
Node7	-1e7dd24b8f19f2f6f5002f6a928bc34f...	50	22/6/16 1:08 PM
Node8	5b384ce32d8cdef02bc3a139d4cac0a2...	38	22/6/16 1:08 PM
Node9	-14b53cfcc1754ca6e1f0310573d931c0...	78	22/6/16 1:08 PM
Node10	59129aacfb6cebbe2c52f30ef3424209f...	66	22/6/16 1:08 PM
Node11	215bb47da8fac3342b858ac3db09b033...	94	22/6/16 1:08 PM
Node12	286dd552c9bea9a69ecb3759e7b9477...	43	22/6/16 1:08 PM

Figure 5 – Base station containing secure data collected from different sensor nodes

There are many sensor nodes sending temperature details. The data is aggregated and sent to base station. There are probabilities for attackers to inject fault data as well. In such cases the proposed algorithm was able to perform enhanced iterative filtering to handle attacks if any. The attack status is updated as revealed in Figure 6.

e-ISSN: 2394-8299
p-ISSN: 2394-8280



Node Name	Energy	Digital Sign	Temperature	Attacked
Node7	90518	-49a7603954f237d30edf66...	0	Yes
Node8	62911	632667547e7cd3e0466547...	31	No
Node9	94578	-3f8b2afecfd14d46c1daab8...	36	No
Node10	83376	-3a48925c19f72cb124f8db...	53	No
Node11	76432	31bd9b9f5f7b338e41b5618...	98	No
Node12	81497	-41b9e5f32e025fad5963c0...	84	No

Figure 6 – Attack status

Different nodes and their energy levels are revealed. The other data is related to temperature besides showing the attack information. The iterative filtering process can judge the values to know whether they are genuine and make well informed decisions.

CONCLUSIONS AND FUTURE WORK

In this paper we studied secure data aggregation. The review of literature found that there are many techniques available. IF algorithms are widely used for secure data aggregation. However, they are not adequate to handle collusion attacks. In other words, WSNs are vulnerable to such attacks. In this paper we proposed and implemented an enhanced iterative filtering algorithm that performs modelling of data and updates it every time iteratively. It can thus predict the data by comparing the model and suspect entries injected by adversaries. We built a prototype application that simulates and demonstrates the proof of concept. The application is implemented using Java platform with a Graphical User Interface (GUI) and visualization of WSN. The empirical results revealed that the proposed scheme is effective for secure data aggregation in WSN in presence of collusion attacks. This research can be extended further by considering real time scenarios and implementing the algorithm to evaluate it further.

REFERENCES

[1] H.-S. Lim, Y.-S. Moon, and E. Bertino, “Provenance-based trustworthiness assessment in sensor networks,” in Proc. 7th Int. Workshop Data Manage. Sensor Netw., 2010, pp. 2–7.
[2] R.-H. Li, J. X. Yu, X. Huang, and H. Cheng, “Robust reputationbased ranking on bipartite rating networks,” in Proc. SIAM Int. Conf. Data Mining, 2012, pp. 612–623.
[3] E. Ayday, H. Lee, and F. Fekri, “An iterative algorithm for trust and reputation management,” Proc. IEEE Int. Conf. Symp. Inf. Theory, vol. 3, 2009, pp. 2051–2055.
[4] H. Liao, G. Cimini, and M. Medo, “Measuring quality, reputation and trust in online communities,” in Proc. 20th Int. Conf. Found. Intell. Syst., Aug. 2012, pp. 405–414.
[5] B.-C. Chen, J. Guo, B. Tseng, and J. Yang, “User reputation in a comment rating environment,” in Proc. 17th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, 2011, pp. 159–167.
[6] H.-S. Lim, G. Ghinita, E. Bertino, and M. Kantarcioglu, “A gametheoretic approach for high-assurance of data trustworthiness in sensor networks,” in Proc. IEEE 28th Int. Conf. Data Eng., Apr. 2012, pp. 1192–1203.
[7] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, “Reputationbased framework for high

integrity sensor networks," ACM Trans. Sens. Netw., vol. 4, no. 3, pp. 15:1–15:37, Jun. 2008.
[8] X.-Y. Xiao, W.-C. Peng, C.-C. Hung, and W.-C. Lee, "Using SensorRanks for in-network detection of faulty readings in wireless sensor networks," in Proc. 6th ACM Int. Workshop Data Eng. Wireless Mobile Access, 2007, pp. 1–8.
[9] M. Li, D. Ganesan, and P. Shenoy, "PRESTO: Feedback-driven data management in sensor networks," in Proc. 3rd Conf. Netw. Syst. Des. Implementation, vol.3, 2006, pp. 23–23.
[10] Y. Sun, H. Luo, and S. K. Das, "A trust-based framework for faulttolerant data aggregation in wireless multimedia sensor networks," IEEE Trans. Dependable Secure Comput., vol. 9, no. 6, pp. 785–797, Nov. 2012.
[11] L.-A. Tang, X. Yu, S. Kim, J. Han, C.-C. Hung, and W.-C. Peng, "Tru-Alarm: Trustworthiness analysis of sensor networks in cyber-physical systems," in Proc. IEEE Int. Conf. Data Mining, 2010, pp. 1079–1084.
[12] J.-W. Ho, M. Wright, and S. Das, "ZoneTrust: Fast zone-based node compromise detection and revocation in wireless sensor networks using sequential hypothesis testing," IEEE Trans. Dependable Secure Comput., vol. 9, no. 4, pp. 494–511, Jul./Aug. 2012.
[13] S. Ozdemir and H. C¸ am, "Integration of false data detection with data aggregation and confidential transmission in wireless sensor networks," IEEE/ACM Trans. Netw., vol. 18, no. 3, pp. 736–749, Jun. 2010.
[14] Sriramoju, Ajay Babu. "Analysis on Lossless Image Compression in Image Processing" (2011).
[15] Sriramoju Ajay, B. (2017). INTELLIGENT MOBILE APP FOR FINDING PATH AND TRACKING POST PACKETS USING ANDROID PLATFORM. International Journal Of Research In Science & Engineering, 3(2), 9.
[16] Sriramoju Ajay, B. (2017). Investigation of Feasible Tourist Destinations using Android Mobile App. International Journal Of Research In Science & Engineering, 3(2), 9.
[17] Babu, Sriramoju Ajay, and Namavaram Vijay. "Image Tag Ranking for Efficient Matching and Retrieval." (2016).
[18] Babu, Sriramoju Ajay, and Namavaram Vijay. "Design and Implementation of a Framework for Image Search Reranking." (2016).
[19] Babu, Sriramoju Ajay and Babu, S Shoban. "International Journal of Research and Applications Jan-Mar© 2016 Transactions 3 (9): 422-426 eISSN: 2349–0020."
[20] Babu, Sriramoju Ajay. "PARTICLE SWARM OPTIMIZATION ALGORITHM FOR ROUTING NETWORK" (2017).
[21] Babu, Sriramoju Ajay. "MODIFICATION AFFINE CIPHERS ALGORITHM FOR CRYPTOGRAPHY PASSWORD" (2017).
[22] Babu, Sriramoju Ajay. "Perceptual-Based Quality Metrics For Image and Video Services" (2015).
[23] Sriramoju, Ajay Babu. "Analysis on Image Compression Using Bit-Plane Separation Method" (2014).
[24] Babu, Sriramoju Ajay. "Objective Quality Metric Design For Wireless Image and Video Communication" (2014).
[25] Ajay Babu Sriramoju, Dr. S. Shoban Babu. "Study of Multiplexing Space and Focal Surfaces and Automultiscopic Displays For Image Processing" (2013).
[26] Sriramoju, Ajay Babu. "Image Processing: Lossy Compression by Color Quantization and Gct Modeling" (2012).