A Heterogeneous Framework to Detect Intruder Attacks in Wireless Sensor Networks

Mustafa Al-Fayoumi
Computer Science Department
Prince Sattam bin Abdulaziz University, KSA
Princess Sumaya University for Technology
(PSUT), Amman, Jordan

Yasir Ahmad
Computer Science Department
Prince Sattam bin Abdulaziz University
Riyadh,
Saudi Arabia

Usman Tariq
Information Systems Department
Prince Sattam bin Abdulaziz University
Riyadh,
Saudi Arabia

***Abstract*—Wireless sensor network (WSN) has been broadly implemented in real world applications, such as monitoring of forest fire, military targets detection, medical and/or science areas and above all in our daily home life as well. Nevertheless, WSNs are effortlessly compromised by adversaries due to their broadcast transmission medium as a means of communication which are lacking in tamper resistance. Consequently, an intruder can over hear all traffic, replay previous messages, inject malicious data packets, or can compromise a node. Commonly, sensor nodes are very much vulnerable of two main issues in security aspect that are node authentication and compromising a node. In this paper, a heterogeneous framework of node capture and intrusion detection for WSNs is proposed. This framework efficiently detects the captured nodes by using a novel technique, embedded with an Intrusion Detection mechanism which aggregates Signature and Anomaly based approach with Neural Network Multi-Layer Perceptron (MLP) classification in a clustering environment. Moreover, the proposed framework achieves efficiency at reasonable computation and communication costs and it can be a security shield to real WSN applications.**

***Keywords*—Intrusion; node compromise; anomaly; signature; MLP**

I. INTRODUCTION

Sensor networks are immensely distributive networks of tiny, light-weight wireless nodes, deployed in huge numbers for the monitoring of environment by the calculation of physical parameters e.g., pressure, temperature, or relative humidity. The current advances in (MEMS) Micro electro mechanical systems technology made possible to build sensors [1]. Some of the important applications of wireless sensor networks are as follows:

- Wireless sensor networks could be an essential part of military command, computing control, communications, surveillance, intelligence, and targeting systems [2].
- Sensor networks are also largely applied in agriculture research, habitat monitoring, fire detection and traffic management [3].
- Sensor networks are extensively used in home appliances, health care, classroom operations, and structural monitoring [4-8]

The topology design in the WSNs differs from an easy star network to a complex wireless multi-hop mesh network. Data propagation technique used in between the different network hops could be flooding or routing. Conventional WSNs are susceptible to various kinds of attacks. These attacks could be typically classified into following types [9-10]: (i) attack on the authentication and secrecy, (ii) attack on availability of the network, and (iii) hidden attacks on service integrity. The focus of this paper is on the first and third types of attacks on sensor networks. Currently, security mechanisms for sensor networks focus on external attacks, and these mechanisms fails to protect internal attacks where a group of sensor nodes being compromised. In hidden attacks, an intruder tries to compromise a sensor node so as to inject fake data. In this form of attack, an intruder accesses the codes and encryption keys utilized by the network. The adversary can constantly interrupt or halt the normal functions of the sensor network e.g., building routing loops. A compromised node might impact the sensor network by sending the authenticated data to the base station. By physically accessing the sensor nodes an intruder can fully control the operations of few sensor nodes. Compromising a node is normally contemplated as one of a most challenging problem in WSN security [11].

An adversary attacking a node tries straightaway to tamper the captured node physically to retrieve the cryptographic information. This attack can harm the security in the architecture of the underlying network. Furthermore, it can possibly increase many consecutive power-full insider threats [12]. Once compromised by an adversary, the node can perform variety of tasks which it is commanded to do. The node can be directed to be a launch pad for spam posting, stealing private information, or spread spyware. Considering the operation of a WSN depends on the accuracy of the secret information exchanged between the nodes, the node compromise poses detrimental impact in WSNs. Consequently, a single compromised node could be a mighty weapon for an adversary in WSNs.

Since, wireless communication is susceptible to eavesdropping, an intruder can oversee the flow of data and tries to modify, intercept, disrupt, or falsify data packets [13] and disseminates incorrect information to the sink. Typically, sensor nodes have scarce resources and short transmission range, an intruder possessing huge processing capability and farther range of communication could compromise many sensors at a time in order to modify the real data during communication.

A large number of security relevant solutions are previously proposed e.g., exchanging the key, authentication, secure routing, safety mechanisms for particular attacks. To some level these security techniques are able to ensure the security; however, they can't remove the security attacks completely [14]. To overwhelm the challenge faced by WSNs, this paper proposes a scheme which efficiently detects the captured nodes by using a novel technique, embedded with an Intrusion Detection mechanism which utilizes Anomaly and Signature based approach in the combination of Clustering, and Neural Network Multi-Layer Perceptron (MLP) classification algorithm [15].

The remaining parts of this paper are organized as follows: Section 2, gives the literature review and related works. Section 3 describes the framework with details of algorithms of the proposed solution. The experimental results are demonstrated in section 4. The paper is concluded in section 5.

II. Literature Review

In [9] the authors propose 'software based attestation for embedded devices' (SWATT) to discover an immediate change in the content of sensor memory which indicates the chance of an attack.

In [16], Hartung et. al., retrieve the cryptography secrets on a sensor node of MICA2 type by removing its inner memory via the JTAG interface. This attack is further explored in [17], where Becher et. al., displays how to retrieve many components of node hardware like external memory, and the boot-strap loader or the JTAG-interface. The authors suggested that the programming interfaces should be disabled so that un-authorized access to the microcontroller is prevented. They also indicated that if the node is captured it certainly remains absent for a considerable period which is enough to figure out node captivity.

[18] presents an absolute distributed-detection system which cooperates with nearest node(s) to yield a decision regarding the malicious behavior of the sensors. The authors enhance the starting security framework and develop a more promising Intrusion Detection System agent architecture which is known as LIDeA (lightweight-intrusion detection architecture) in [19]. They proposed a new encryption scheme which secures the network from external attacks and also devised few rules to detect sinkhole attack. They focused on MintRoute-routing protocol, and the approach they proposed is not applicable to the routing protocols like LEACH protocol and more.

In [20] the authors developed an Intrusion Detection system which is based upon SEP (Stable Election Protocol) for clustered-heterogeneous WSNs. The advantage of adopting SEP protocol is its heterogeneity awareness in order to increase the life time of the first node before its death. They trained their system to identify four-types of attacks that are DOS, Probe, R2L, and U2R. Their proposed scheme used the KNN (K-nearest neighbor) classifier to detect an anomaly in the system.

In [21] the authors proposed the IP address, MAC address, and Port Number based intruder sniffing system for cluster-based WSNs. According to them, the proposed approach is truly efficient in energy consumption for initial detection & prevention of security risks and attacks. They argued that initial detection & prevention of the adversary by effective security system restricts several problems such as network slowdown, injecting of fake data, and much more. They also believed that by designing a security mechanism where a Base Station has the responsibility of the overall network security, higher security measures are expected without draining the energy levels of the cluster heads as well as individual sensor nodes.

In [22], Coppolino et.al, has shown a light weight, hybrid and distributed IDS for WSNs. They utilized both anomaly based and misuse based techniques. Their technique consists of a central agent (CA) which carries out an extremely accurate intrusion detection by devising data mining methods and they consider local agents (LA) that are lighter running on motes to detect intrusions.

In [23], Yassine et.al, proposed an IDS model which uses anomaly detection based on SVM technique and a set of attacks that are represented by fixed rule signatures. These signatures are designed to detect the malicious behavior of the intruder by anomaly detection method. This approach is implemented in a cluster based topology to increase the network lifetime.

III. The Proposed Framework

The proposed framework defends the network from various types of attacks on service integrity, authentication and secrecy etc., and at the same time it doesn't depend on a particular routing protocol. The proposed framework is assumed geographic routing with a slight modification in multi-hop topology. In the proposed routing protocol, nodes need to only be aware about the locations of nearest neighbors' in the cluster; through the network the data packets are routed by being forwarded to a cluster. The major advantages of geographic routing over other routing strategies of WSNs include; (i) stateless, and therefore highly energy efficient, nature of routing, (ii) fast adaptability to network's topological changes, and (iii) scalability [24-25] which should be the main objectives while deploying any type of WSN. These distinguished characteristics makes the protocol efficient, simple, and physically deployable, averting the use of practical routing that can originate complexity and also overhead in the mobile framework. The methodology of the proposed framework as follows:

A. Hidden attacks on Service integrity:

The sensor nodes are deployed sparsely in the network. After the deployment the sensors those are physically closer chooses a cluster head unanimously which depends upon

various parameters like battery power etc at the selection time. This selection is dynamic in the sense the node with higher battery power is selected as a CH. The sensors in a cluster dynamically create the node ID lists of the neighboring nodes and the CH. This list is maintained until the nodes changes the cluster itself or by the deployed authority or an adversary who tries to displace/compromise the node. The cluster head is responsible for the data transmission between the clusters which finally arrives to the sink. The deployed sensor reads/senses the data from the environment and disseminates it to the cluster head by applying geographic routing protocol. Then it is the responsibility of the cluster head to transmit the data to another CH or to the sink. This paper proposes an algorithm to prevent the possible node compromise by an adversary:

ALGORITHM 1:

Begin

1) If 'n_1' and any other neighboring node 'n_2' talks to each other (by transmitting messages) after a specified interval of time about their presence and non-compromising behavior in the network. Two cases arise about this scenario:

a) If a node 'n_1' is not sending the message to its neighboring nodes due to some other reason except node compromise in the specified period of time say 't', there may be many possible reasons like traffic congestion, re-configuring its hardware etc.

b) If a node 'n_1' is compromised, the neighboring node 'n_2' waits for the message for a specified period of time say 't', and then broadcasts the failure mode of node 'n_1' all the neighboring node blocks the node *ID* in their lists temporarily for a certain threshold time 'T'. When the compromised node doesn't acknowledge its presence after the expiration of the threshold is blocked permanently and black listed from the network.

2) If an adversary tries to shift the location of any particular node(s) from the deployed area so as to compromise its immediate neighboring node ID list, retrieve the cryptographic keys etc. Two cases arise:

a) The attacked node senses the displacement by an unauthorized authority without a certain predefined verification shuts down the system immediately and erases its memory and node ID list.

b) The displaced node before shutting the system down raises an alarm and notifies about the attack to the neighboring nodes and the CH.

End

Below is the flow chart representation of proposed node compromise algorithm, as shown in Fig. 1.

B. Attack on the authentication and the secrecy:

An Intrusion Detection System is one potential resolution for several security attacks in WSNs. IDS can only detect the attacks but are unable to prevent them. Once detected, the IDSs can raise an alarm to apprise the controller to take appropriate action. The standard classification of intrusion in networks fall into four major categories: DoS, Probe, U2R and R2L Two main classes of IDSs exists. (1) rule based IDS and (2) anomaly based IDS [26]. Rule based or signature based IDs is used for the detection of intrusions with the assistance of built in signatures. Rule based IDS has the ability to detect known attacks with greater accuracy, however, it is not able to detect attacks that are new and for which there are no signatures present in the intrusion database. Whereas, Anomaly based IDSs are able to detect new and novel intrusions using the matching of routine traffic patterns and/or resource utilizations.

For authentication and secure data transmission in the wireless sensor network, a hybrid Intrusion Detection System, anomaly & Signature based is proposed. The proposed IDS scheme is also distributed in the following way; (i) misuse based IDS are implemented locally in the nodes. The network is trained to detect several types of known attacks before the deployment phase, and the signatures are added in the nodes profile. This misuse (signature) based IDS is a light weight scheme and is used to detect known attacks on the network.

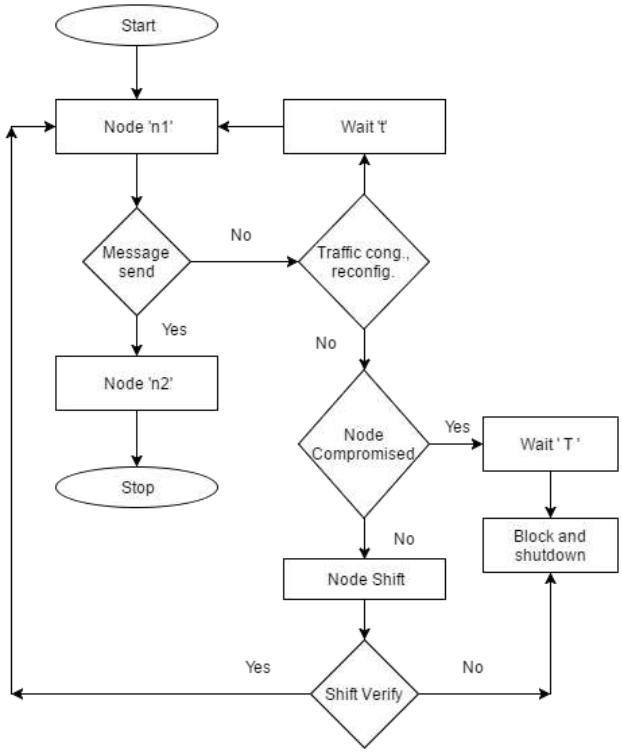

Fig. 1. Algorith #1 Flowchart

In case of new or novel attacks which can't be detected by the signature based scheme in the sensor nodes, (ii) anomaly based IDS which is implemented in the CHs comes into action. Anomaly based IDS scheme in the CHs detects any deviation from the normal functioning of the network. If a deviation is being detected, the CH immediately stops the transmission of data and informs the neighboring CHs by raising some kind of alarm. Simultaneously, the new signature pattern which is based on this deviation is added to the misuse based IDS profile in the sensor nodes for future detection.

In this way, both the IDS techniques are utilized in a very efficient and optimal manner. This technique makes the proposed network robust and secure from several kinds of

intruder attacks. This scheme is basically a blend of stand-alone and hierarchical architecture in WSNs. The proposed IDS scheme has an advantage over the monitoring node schemes in the literature, IDS is implemented in all the sensor nodes which makes them self-dependable to resist any kind of attack to a large extent, and at the same time not to rely on any other monitoring node for the intrusion detection purpose, which if compromised disrupts all the network functionality.

C. Anomaly based detection model:

This model is proposed to implement the Multi-Layer Perceptron (MLP) (Fig. 2) and the backpropagation algorithm for the training of anomaly based detection system. It is a supervised learning algorithm [27]. The MLP is an artificial neural network which is extensively used to solve different problems like pattern recognition, digression etc. Multi-layer Perceptron is a network that is composed of several neurons, which are divided into input layer, output layer, and one or more hidden layers. The function that connects the input and the target output is what the perceptron must find. The way it accomplishes this is by this very simple rule:

$$y_i = f\left(\sum_{j=1}^{m} w_{ij}\, x_j + b_i\right) \qquad (1)$$

Equation (1) calculates y_i which is the output of the node, w denotes the vector of weights, x is the vector of inputs, b is the bias and f is the activation function.

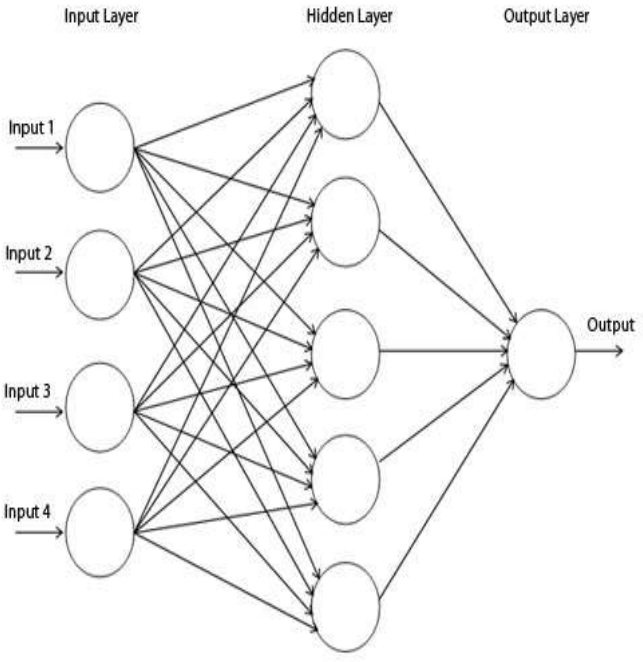

Fig. 2. MLP Diagram

Design: In this case, the proposed IDS consist of several neural networks which operate in parallel [28]. Every CH is a three-layer neural network and has its own training data sets for intrusion detection. The back-propagation algorithm is used to train the individual CH nodes. The parameters were implemented are listed below:

- Back propagation algorithm used for CH IDS learning.
- MLP structure is utilized with input, hidden, and output layers.
- Learning rate is set to η (0.1 – 1.0).
- Sigmoid function is used as activation function.

The MLP algorithm which is implemented in CHs for anomaly based IDS is defined as follows:

ALGORITHM 2:

Begin

- Initialize weights at random, choose a learning rate η
- Train the network for each training example (input pattern and target output (*s*)):

  Do - Until output is produced:

  Do - forward pass through network layer by layer:

  - Apply Inputs
  - Multiply by weights
  - Sum up the outputs
  - Apply sigmoid activation function
  - Pass the output to next layer
- Done
  - Compute error (delta or local gradient) for each output unit δk
  - By backpropagation Layer-by-layer, compute error (delta or local gradient) for each hidden unit δj
  - Correct the output layer of weights.
  - Correct the input weights.
  - Update all the weights Δwij
- Done

End

Below is the flow chart representation of the proposed anomaly detection (MLP) algorithm, as shown in Fig. 3.

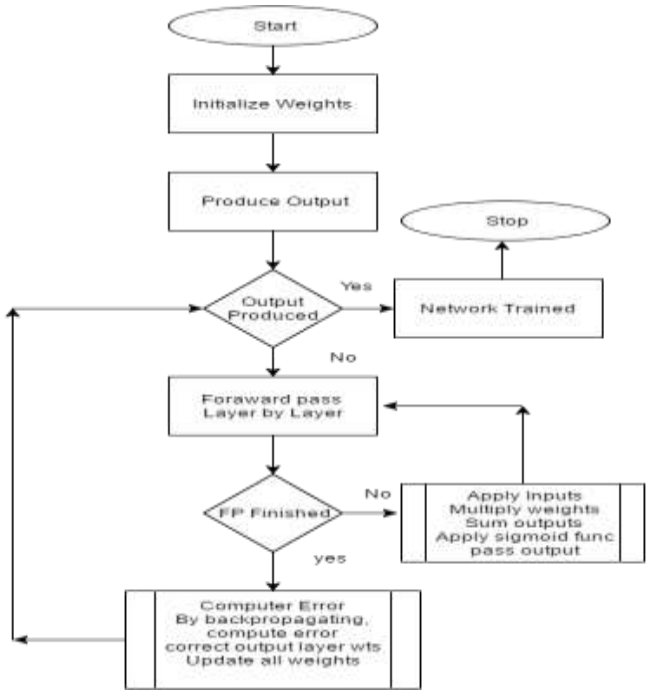

Fig. 3. Algorithm #2 Flowchart

The structure of neural networks and WSNs has similar characteristics i.e., inter-connected components. Both types of networks implement functions which maps the input values to the output values. Artificial neural networks (ANN) have general characteristics which are desirable in WSNs also. The selection of ANN MLP classification algorithm for the training of anomaly based detection in CHs has many reasons which are defined as under:

- This technique is designed to be parallelized.
- It is very fast to evaluate new attacks.
- It is also robust on noisy training data which is inherent in WSNs.

MLP classifies the data into five categories which are Normal, Probe, DoS, U2R, and R2L.This approach reduces the (FA) false alarm at the same time maintains accuracy and detection at higher range. With respect to previous researches in intrusion detection, the performance of IDS is calculated and evaluated by measure of accuracy, detection rate and false alarm which are defined in the "(2)", "(3)" and "(4)" as follows:

$$Accuracy\ (A) = TP + TN/(TP + TN + FP + FN) \quad (2)$$

$$Detection\ Rate\ (DR)\ =\ TP/\ (TP + FP) \quad (3)$$

$$False\ Alarm\ (FA)\ =\ FP/\ (FP + TN) \quad (4)$$

IV. Experimental Results

The performed experiments have been conducted to evaluate the proposed framework in terms of accuracy, attack detection rate and false alarm. The evaluation of proposed IDS detection system is conducted using KDD Cup 99 dataset [29]. The specified dataset is denounced for repetition of records. This repetition of records precludes the learning algorithms to detect unknown attacks [30]. Notwithstanding, it is the only publicly available labelled dataset which has been used extensively in the research field of intrusion detection. By experiments the proposed approach on KDD Cup 99 dataset provides a significant evaluation and makes the performance comparison with other advanced technique proportionate.

Two experiments have been carried out on MLP classifier and SVM using the KDD Cup'99 dataset. All experiments were performed on an Intel® core™ 2 Duo CPU T7500 @2.20 as computing machine with the following specifications: 4 GB main memory, and running Microsoft Windows 8. During the evaluation, the 10 percent labeled data of KDD Cup 99 dataset is utilized, where three types of legal traffic (TCP, UDP and ICMP) are available.

The evaluation of these experiments is based in terms of accuracy, attack detection rate and false alarm. Fig. 4 classifies the result for each type of data using testing dataset. Data from Table 1 is represented graphically in Fig. 5 which clearly shows that for the given attack categories, MLP performs better than K-M algorithm. Moreover, the data collected from Table 2 which is represented in Fig. 6 shows that in detecting false alarm MLP lags behind only in the probing category. MLP shows better detection performance more than 85% of attack records for probing category, more than 95% in DoS and more than 97% in R2L category.

TABLE I. Detection Probability of Attacks

Comparison Criteria	**Approaches**	
	MLP	***K-M***
Probe	0.887	0.876
DoS	0.973	0.973
U2R	0.298	0.298
R2L	0.096	0.064

TABLE II. Detection Probability of False Alarms

Comparison Criteria	**Approaches**	
	MLP	***K-M***
Probe	0.004	0.026
DoS	0.004	0.004
U2R	0.004	0.004
R2L	0.003	0.001

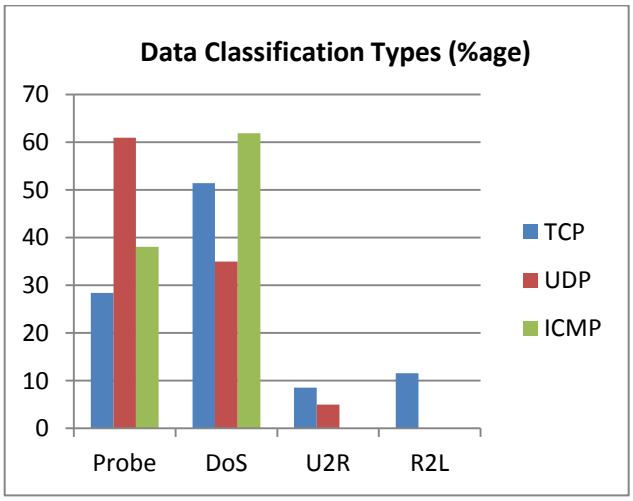

Fig. 4. Result of different classification Data types (Testing Dataset)

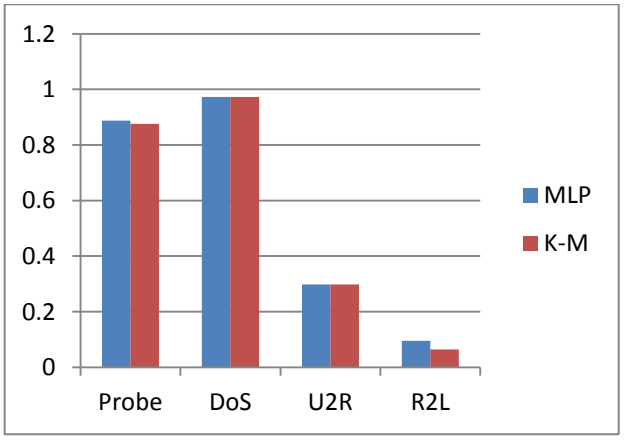

Fig. 5. Comparison of Detection probability of different Attacks

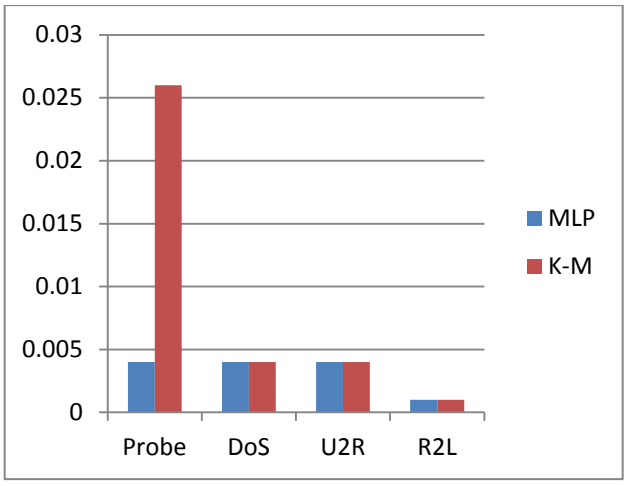

Fig. 6. Comparison of Detection probability of False Alarm

The Fig. 7 and 8 represent how different types of data (PN=Predicted Normal; PA=Predicted Attack) are classified by MLP network using the testing data set. As it can be seen clearly in Fig. 7 and 8 MLP Neural Network resulted fewer false positives and Negatives.

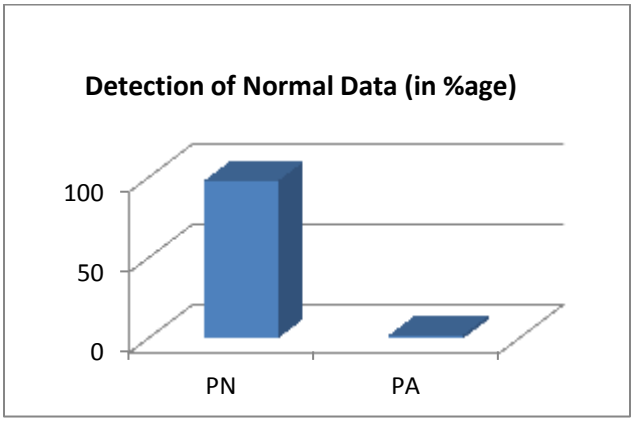

Fig. 7. Detection of Normal Data (Testing Dataset)

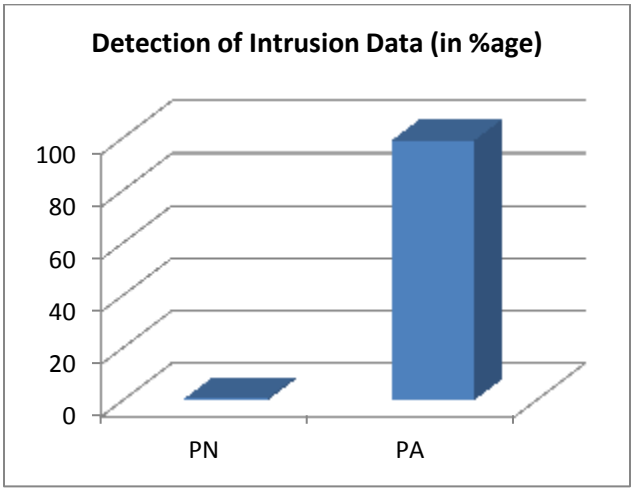

Fig. 8. Detection of Intrusion Data (Testing Dataset)

V. Conclusion and Future Work

The proposed framework aims to protect the network from the attacks on service integrity, authentication and secrecy by employing a heterogeneous approach of intrusion detection. A heterogeneous IDS framework which utilizes many state-of-the-art approaches together to achieve the maximum probability of intrusion detection in WSNs. The different experiments which were carried out in comparison with K-M algorithm evaluates the performance of proposed technique of IDS on the KDD 1999 Cup dataset which showed that MLP detects more than 85% of attack records for probing category, more than 95% in DoS and also more than 97% in R2L category. It also showed promising results in detecting false alarms. In future, will be considered some more innovative techniques for intrusion detection in WSNs.

Acknowledgment

This project was supported by the deanship of scientific research at Prince Sattam bin Abdulaziz University under the research project # 2015/01/4646.

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks," IEEE Communications Magazine, vol. 40, no. 8, pp. 102-116, August 2002.

[2] Chee-Yee Chong, S.P. Kumar, "Sensor networks: evolution, opportunities, and challenges," Proceedings of the IEEE, vol.91, no.8, pp.1247,1256, Aug. 2003 doi: 10.11 09/ JPROC.2003.814918.

[3] K. Martinez, J. K. Hart and R. Ong, "Environmental sensor networks," IEEE Computer, vol. 37, no. 8, pp. 50-56, Aug. 2004. doi: 10.1109/MC.2004.91.

[4] L. Schwiebert, S.D.S. Gupta, J. Weinmann, "Research challenges in wireless networks of biomedical sensors," 7th annual international conference on Mobile computing and networking, (MobiCom2001), pp.151-165, July 2001, Rome, Italy. doi:10.1145/381677.381692.

[5] G. Amato, S. Chessa, F. Conforti, A. Macerata, C. Marchesi, "Health Care Monitoring of Mobile Patients," ERCIM News No. 60 pp. 69-70, January 2005.

[6] I. A. Essa, "Ubiquitous sensing for smart and aware environments," IEEE Personal Communications, vol. 7, no. 5, pp. 47-49, Oct 2000. doi: 10.1109/98.878538

[7] M. Srivastava, R. Muntz, M. Potkonjak, 2001. "Smart Kindergarten: Sensor-based Wireless Networks for Smart Developmental Problem-solving Environments," 7th Annual Int. Conf. on Mobile Computing and Networking (MobiCom2001), pp.132–138 July 2001, Rome, Italy. doi: 10.1145/381677..381690.

[8] N. Xu, S. Rangwala, K.K. Chintalapudi, D.Ganesan, A. Broad, R. Govindan, D. Estrin, "A Wireless Sensor Network for Structural Monitoring," SenSys '04 Proceedings of the 2nd international conference on Embedded networked sensor systems, Baltimore,MD,USA, , pp.13–24, November 20014. doi:10.1145/1031495.1031498.

[9] P. Adrian, S. John, W. David, "Security in wireless sensor networks, "Communications of the ACM" vol. 47 no.6, June 2004. doi: 10.1145/990680.990707..

[10] W. Wei, Q. Xu, L. Wang, X.H. Hei, P. Shen, W.Shi, L.Shan, "GI/Geom/1 queue based on communication model for mesh networks," International Journal of Communication Systems, vol. 27, no. 11, pp. 3013-3029, 2014.

[11] C. Krauß, M. Schneider, C. Eckert, "On handling insider attacks in wireless sensor networks," Information Security Technical Report, vol. 13, no. 3, pp. 165–172, 2008.

[12] C.P. Pfleeger, S.L. Pfleeger, Security in Computing, 3rd edition, Prentice Hall 2003.

[13] Y. Ping, J. Xinghao, W. Yue, and L. Ning, "Distributed intrusion detection for mobile ad hoc networks," Journal of Systems Engineering and Electronics, vol. 19, no. 4, pp. 851–859, 2008.

[14] C. Hartung, J. Balasalle, R. Han, "Node Compromise in Sensor Networks: The Need for Secure Systems," CU-CS-990-05. Computer Science Technical Report, Paper 926, January 2005. http://scholar.colorado.edu/csci_techreports/926.

[15] W. Wei, X.L. Yang, P.Y. Shen, B. Zhou, "Holes detection in anisotropic sensornets: Topological methods," International Journal of Distributed Sensor Networks, vol. 2012, pp. 1-9, 2012. doi:10.1155/2012/135054.

[16] B. lexander, B.Zinaida, D. Maximillian, "Tampering with motes: real-world physical attacks on wireless sensor networks," Third international conference on Security in Pervasive Computing, pp 104-118, York, UK, April 2006. doi: 10.1007/11734666_9.

[17] I. Krontiris, T. Dimitriou, "Towards intrusion detection in wireless sensor networks," 13th European wireless conference, Paris, 2007.

[18] L. Krontiris, T. Dimitriou, T. Giannetsos, "LIDeA: A distributed lightweight intrusion detection architecture for sensor networks," 4th International Conference on Security and Privacy in Communication Netowrks, pp. 1-10, September 2008, [SecureComm '08, Istanbul, Turkey]. doi:10.1145/1460877.1460903.

[19] A. Manal, A. Ebtesam, A. Nada, "Energy Efficient Cluster-Based Intrusion Detection System for Wireless Sensor Networks," International Journal of Advanced Computer Science and Applications (IJACSA), vol. 5, no. 9, 2014.

[20] S.S. Patil, P. S. Khanagoudar. "Intrusion Detection Based Security Solution for Cluster Based WSN," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), vol.1 no.4, pp: 331-340, 2012.

[21] L. Coppolino, S. D'Antonio, A. Garofalo, L. Romano, "Applying data mining techniques to intrusion detection in wireless sensor networks," Eighth International Conference on, P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), pp. 247-254, October 2103. doi: 10.1109/3PGCIC.2013.43

[22] M. Yassine, A. Ezzati, Y. Qasmaoui, M. Mbida, "A Global Hybrid Intrusion Detection System for Wireless Sensor Networks," Procedia Computer Science, vol. 52, pp. 1047-1052, 2015.

[23] Feng Zhao, Leonidas Guibas, Wireless Sensor Networks: An Information Processing Approach, Morgan Kaufmann Publishers Inc., San Francisco, CA, 2004.

[24] M.R. Norouzian, S. Merati, "Classifying Attacks in a Network Intrusion Detection System Based on Artificial Neural Networks," Conference Advanced Communication Technology (ICACT), 13th International Conference on Publication, pp. 868 – 873, 2011.

[25] S. Sahin, Y. Becerikli, and S. Yazici, "Neural Network Implementation in Hardware Using FPGAs," Neural Information Processing, Lecture notes in Computer Science, Berlin Germany: Springer, vol. 4234, 2006.

[26] S. J. Stolfo, W. Fan, W. Lee, A. Prodromidis, and P. K. Chan, "Costbased modeling for fraud and intrusion detection: results from the JAM project," The DARPA Information Survivability Conference and Exposition 2000 (DISCEX '00), Vol.2, pp. 130-144, 2000.

[27] W. Wang, X. Zhang, S. Gombault, and S. J. Knapskog, "Attribute Normalization in Network Intrusion Detection," The 10th International Symposium on Pervasive Systems, Algorithms, and Networks (ISPAN), 2009, pp. 448-453.

[28] W. Wei, Y. Qi, "Information potential fields navigation in wireless Ad-Hoc sensor networks," Sensors, vol. 1, no. 5, pp. 4794-4807, 2011.

[29] H. Song, M. Brandt-Pearce, "A 2-D discrete-time model of physical impairments in wavelength-division multiplexing systems," Journal of Lightwave Technology, vol. 30, no. 5, pp. 713-726, 2012. doi: 10.1109/JLT.2011.2180360.

[30] H. Song, M. Brandt-Pearce, "Range of influence and impact of physical impairments in long-haul DWDM systems," Journal of Lightwave Technology, vol. 31, no. 6, pp. 846-854, March 2013. doi: 10.1109/JLT.2012.2235409.

[31] H. Song, M. Brandt-Pearce, "Model-centric nonlinear equalizer for coherent long-haul fiber-optic communication systems," 2013 IEEE Global Communications Conference (GLOBECOM), pp. 2394-2399, Atlanta, GA, 2013. doi: 10.1109/GLOCOM.2013.6831432.

[32] H. Song, M. Brandt-Pearce, "A 2-D discrete-time model of physical impairments in wavelength-division multiplexing systems," Journal of Lightwave Technology, vol. 30, no. 5, pp. 713-726, 2012. doi: 10.1109/JLT.2011.2180360.

[33] H. Song, M. Brandt-Pearce, "Range of influence and impact of physical impairments in long-haul DWDM systems," Journal of Lightwave Technology, vol. 31, no. 6, pp. 846-854, March 2013. doi: 10.1109/JLT.2012.2235409.

[34] H. Song, M. Brandt-Pearce, "Model-centric nonlinear equalizer for coherent long-haul fiber-optic communication systems," 2013 IEEE Global Communications Conference (GLOBECOM), pp. 2394-2399, Atlanta, GA, 2013. doi: 10.1109/GLOCOM.2013.6831432.