Security of Wireless Sensor Networks Employing Malicious Node Detection & Prevention Method

Aditya Dwivedi [1], Apurva Sharma [2], Anchal Yadav [3], Rizwan Khan [4]
[1, 2, 3] Dept of Computer Science Engineering
[4]Assistant Professor, Dept of Computer Science Engineering
[1, 2, 3, 4] ABES Institute of Technology, Ghaziabad, 226031, India

Abstract- *The comprehensive impetus of conferring this research paper is to focus upon the security of the communication through the wireless networks all around the world. The communication between the sender and receiver taking place over a wireless based network is very much vulnerable to the different types of active and passive attacks. The main concern here is the active attack in which the attacker tends to steal or get the data/message signal which is being transmitted over the network and then destroy the data, or introduce the false data, or alter/modify the data. The proposal of the approach is based on developing an evolved IDS (intrusion detection system) [1] in order to detect the attacks by encountering the malicious and harmful node as early as possible in the network so as to protect the data from the attacker. After getting through various advanced technology it has been found that if the IDS get trained with the help of an ANN (Artificial Neural Network) in order to identify the major harmful attacks like black-hole attack, grey-hole attack, scheduling attack and flooding attack which are types of DoS (Denial-of-Service) [2] active attack then it would be a lot easier and helpful to secure and defend the network from such attacks as well as the data.*

Keywords- WSN, security, IDS, ANN, DoS attack.

I. INTRODUCTION

The security of data is the top most priority in any data communication. in the WSNs (Wireless Sensor Networks) [3] which is now being implemented in various fields and activities as one of a useful advanced technology, there is a large number of sensor nodes which senses the incoming input signals from the environment and transmit to the gateway of the network which further converts that sensor data into the appropriately expected and acceptable form at the receiving end of the network. The wireless networks are very high in potential [4] as they can be employed even in the area or region where the humans cannot reach easily and also provide the data communication in a wide range through its large network of interconnected sensor nodes.

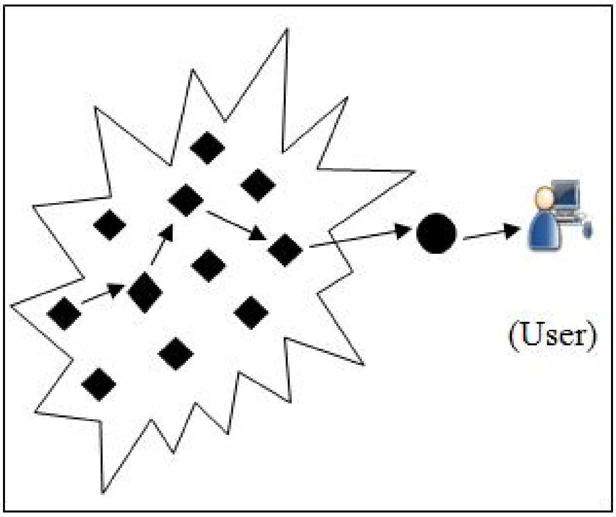


Fig.1: Wireless Sensor Network

◆ These are the sensor nodes.
● This is the Gateway node.

These WSNs has a varying number of self-governing nodes through which the data transmits directed by a more powerful node called as sink node or base node (base station) [5] consequently, it makes it very crucial to fortify the network to sustain its reliability and validity. The premier properties of a WSN is that the nodes are self-governing, self-organizing and there is no central node [6], and a large-scale application.

The limitation and the constraints of a WSN are like low storage of the node, energy requirements, memory limitations [7] and costly communication. But the major threat to any WSN is the various attacks (active or passive). The passive attack in which the attacker monitors the data whereas the active attack in which the attacker attempts to modify the data. In this proposal we are focused on the active attack specifically the denial-of-service attack (DoS). A denial-of-service attack is a security breaching act that takes place when the attacker does not let the legitimate and authenticated users to access the computer systems, network resources and other devices.

In the wireless communication networks, there are various types of denial-of-service attacks: black-hole attack, grey-hole attack, flood attack and scheduling attack.

1. The black-hole attack in which a router which is supposed to convey the data packets turns out to be the one which discards all those data packets and here the attacker pretends to be the cluster head.

2. The grey-hole attack is very much similar to the black-hole attack where the attacker pretends to be the cluster head of other sensor nodes but starts discarding the packet after sometime i nstead intermediately.
3. The flood attack in which the attacker sends the enormous amount of advertising message to affect the functioning of the sensor nodes.

4. The scheduling attack in which the attacker makes the time slot of sending the data by nodes same and hence the scheduling of sending the data by nodes clashes and packets drops.

Since these WSNs are vulnerable to these attacks there are several ways to secure and protect the WSN but the methods to prevent these attacks and other security threats are not sufficient enough to sustain the WSN reliability, then there is a need of alarming system which can be an Intrusion Detection System(IDS) which can play a vital role in identifying and determining the occurrence of the attacks and threats and then notify the nodes to alert them against any strange and abnormal or unusual activity taking place in the network. To make these IDSs functioning properly and serve the main purpose of triggering any abnormal and strange activity which can be a possible threat to the network, there is requirement of training of the IDS which can be performed by considering the Artificial Neural Network(ANN) for decision making purpose.

ANNs are network which are inspired by human brain's neurological system and consist of input layer and output layer with optional number of hidden layer. The purpose of an ANN is to solve the complex problems just like a human brain as well as have the learning capabilities.

ANN can be used to develop a smart and advanced IDS so as to determine, identify, and notify about the occurrence of any threat or attack in the WSN. By evolving an IDS, it would be efficient to trigger the malicious node in the very early stage to avoid the data to be discarded or dropped and also would help to provide the preventive security to the network against the attacks. Although we have several cryptography techniques to protect the data but due to the nature of the network which is distributed and very open and also the limiting features and capabilities of the sensor nodes that is why it becomes even more complex and challenging to provide the essential and needed security to the WSNs just by applying cryptosystems.

II. LITERATURE REVIEW

In the previous work done based on providing the security to the WSNs includes many different models and methods. One of the common way is to apply the cryptography in the WSNs. There are two major types of cryptography as public-key cryptography and private-key cryptography.

In the public-key cryptography or asymmetric key cryptography the encryption key is different from the decryption key and is not shared, like RSA algorithm [8], whereas in the private-key cryptography or symmetric-key cryptography there is only one shared and common key available to perform both the encryption as well as decryption technique, like SHA algorithm. But the major drawback of the cryptography systems being used as a security mechanism in WSNs that this can provide the security and protection only against the attacks which are external by determining the source of packet and content of packet and by performing several functions like hash function [9], private or public key cryptography. So, the cryptography systems are capable of securing the WSNs against the external attacks only by providing the features like authenticating the packets and checking the integrity of the packets.

In the internal attacks where the security keys can be accessed by the attacker and further the attacker can encrypt or decrypt the data to modify or destruct the data, the cryptography systems can't be used to ensure the security against such internal attacks in the WSNs. Therefore, to provide the required and essential security to the WSNs where the mechanism would be able to deal with the internal attacks also is highly needed. One of the most successful way is to employ an IDS in the WSN which will perform all the necessary activities in order to ensure the security of the data packet which is being transmitted from the sender node to receiver node in the network.

The all in all purpose of an Intrusion Detection System is to monitor and analyze the packet transmission in the network and keep looking for any sort of anomalous or deviant activity. After successful detection of any anomaly or irregularity, the IDS is supposed to alarm the user so that the threat or attack can be dealt within the as earliest stage as possible. Most of the IDS has six general components that are:

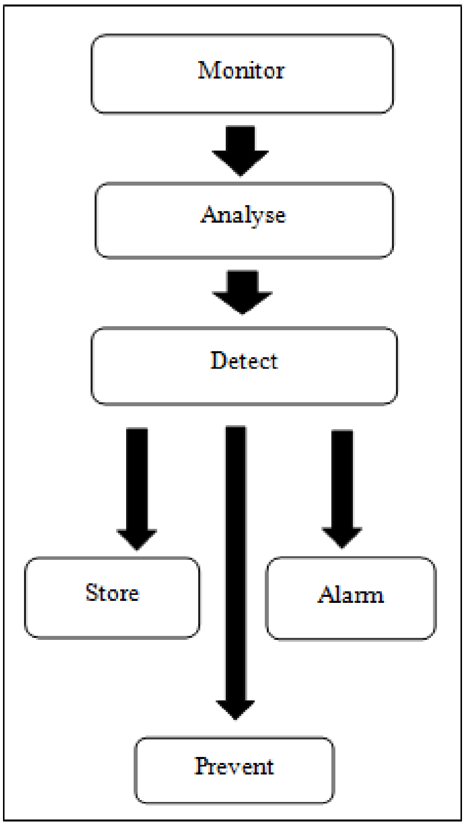


Fig. 2: Components of IDS

- Monitor: This component of an IDS is used to monitor the nearby sensor nodes of the network.
- Analyze: This component in IDS is used for storing the record of normal and abnormal activities and behavior of the sensor nodes for analysis purpose.
- Detect: It is the main component which is used for decision making when the analysis of the network is done, so as to decide whether the node is malicious or not [10].
- Store: It is used for logging operation where packets are stored into a log file for further analysis purpose.
- Alarm: It acts when an intrusion is detected to aware and notify about the detected malicious node.
- Prevent: This component can be added into the IDS to even perform the prevention step when the attack or threat has been detected [11].

All the IDSs which are present at current time are compared and then described by the authors in [11].

In this paper our main purpose is to show an approach in the simplest possible manner which can be used to successfully not only detect the intrusion (malicious node) but also prevent the WSN from that node to protect the data packet.

Section III will describe the method followed, section IV will give description of the procedure, section V shows the result, section VI explaining the future work that can be done, section VII is the conclusion and at last the references.

III. METHOD

To propose the approach as a method to detect and prevent the malicious node in the WSNs the simulation of an WSN is done by using MATLAB. In this approach a matrix of n*n size where n is the no. of sensor nodes present in the wireless network is simulated, then the source node and destination node are declared and initialized randomly. After having the source and destination node, an optimal path is computed and generated by the function to transmit the data in the most efficient way using the optimal path. The heuristic function is used to estimate the closest node position with lowest cost. When the data transmission is started following the optimal cost path computed earlier, the detection of malicious node starts in parallel. As soon as any malicious node is encountered the function will stop the packet transmission and rollback it and then notify with the help of a message box that malicious node has been found, resulting no solution otherwise the transmission takes place successfully.

IV. PROCEDURE

The steps which are involved in our method are as following;

1. Create a wireless network of field size n*n, where ‘n’ is the number of sensor nodes for simulation.

2. Initialize the OPEN and CLOSED sets and their costs by moving in all directions in order of right, left, down and up.

(NOTE: The source node and the goal node are chosen randomly by the method to show the simulation.)

3. Select the nodes from OPEN set with the smallest cost and move towards the neighbor goal node.

4. Put the node in CLOSED set and record its cost.
5. Update OPEN set and their associated costs.

6. For each of the neighbor spaces, assign costs and field pointers and if some are in the CLOSED set with smaller costs, update their costs and pointers.

7. If the node is neither in OPEN nor in CLOSED set, then insert into cost-chart then move pointer and put node in OPEN set.

8. Else the node has already been seen, so now check if we have found a better path to it.

9. Update if we have a better route.

10. If it is not so, then node has already been in CLOSED set, so check to see if have found a better route to it.

11. Find relevant node in CLOSED set.

12. Update if we have a better route.

13. Now, if the element is maximum from member of OPEN set or goal node position index: the solution is found and data will be successfully transmitted.

14. Now find the way back tracing the field pointers starting from goal position only.

15. Plot and display the final path showing the route of packet transmission from source node to goal node.

16. Else no solution is found and obtained that malicious node found and then data packet will not be transmitted to the goal node.

The cost is computed moving in all direction by following the direction in order of right, left, down and up. The simulation of WSN is done in the MATLAB R2016a version.

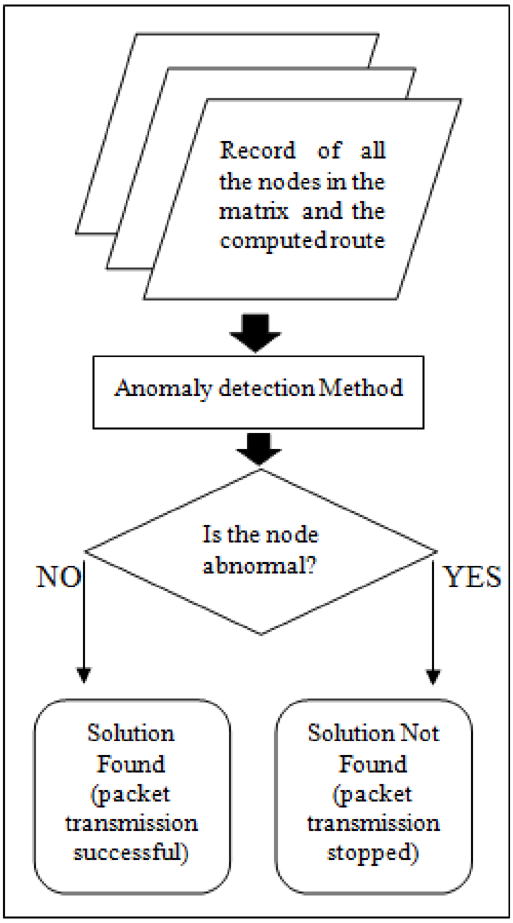

Record of all the nodes in the matrix and the computed route
Anomaly detection Method
Is the node abnormal?
NO
YES
Solution Found (packet transmission successful)
Solution Not Found (packet transmission stopped)

Fig. 3: Flow-chart of anomaly or malicious node Detection.

The code developed is successful in performing two major operation of an IDS which are:

1. To analyze all the nodes between the source node and goal node so as to detect the malicious node in the network before the transmission completes.
2. To prevent the data packet from getting dropped or deviated by halting the transmission process as soon as the malicious node is triggered between the path to goal node.

This code work is also successful in identifying the black-hole attack and grey-hole attack by identifying the malicious node and then is capable of preventing the data from getting attacked, by rolling back the transmission and in the case when no malicious node has been found in the optimal cost path between the source node and goal node, the data is transmitted successfully to the goal node. In this way the developed code work is efficient enough to transmit the data through efficient and optimal route as well as has ability to detect the malicious node and then notify about it and then prevent the data from the attack.

V. RESULTS

The following are the outcomes of the developed code work showing the results of the running code depicting both the cases where CASE-I is where data is transmitted successfully through an optimal cost path computed and CASE-II is where a malicious node has been encountered and then packet transmission is stopped.

We have successfully tested and run the program on the MATLAB (R2016a) platform which is an advanced and high level computing language providing better environment and computation models than other technical languages like C, C++ etcetera. It also provides various other embedded applications and a ton of functions to perform several complex tasks and operations to ease the evaluating and coding process. (NOTE: Green circle is the source node and yellow square is the goal node.

The black region is the depiction of the background wall whereas the white blocks are nodes in the matrix of 10*10 size (n=10). The blocks with varying colors are showing the increment in the progression of the transmission of packet from green source node to yellow goal node by keep looking for the optimal route through all the nearby nodes present in the matrix.)

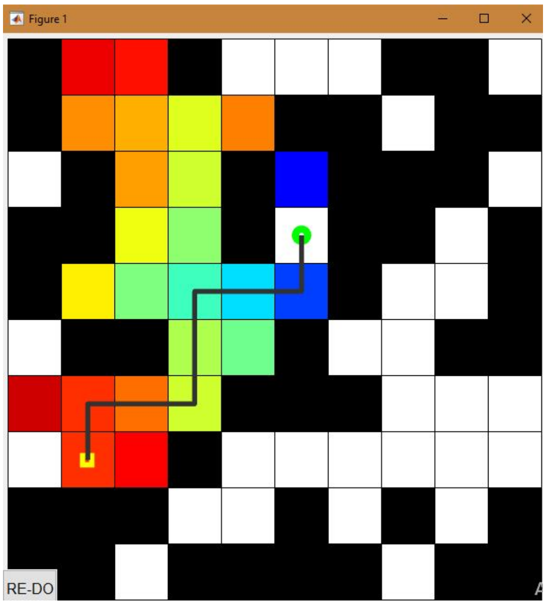


Fig. 4: CASE-I → Solution found and data transmitted successfully.

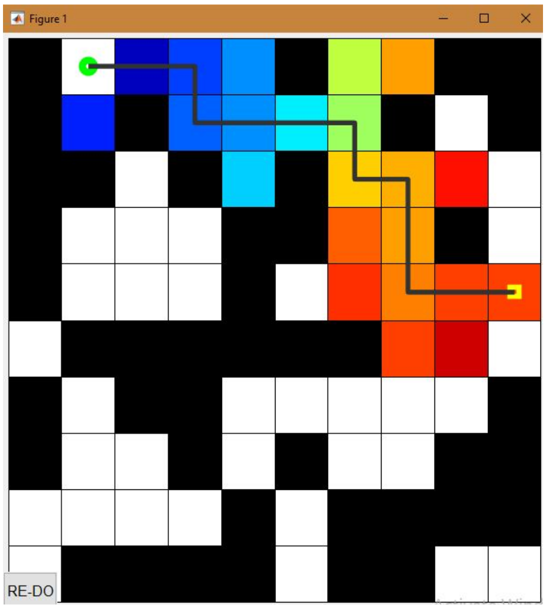
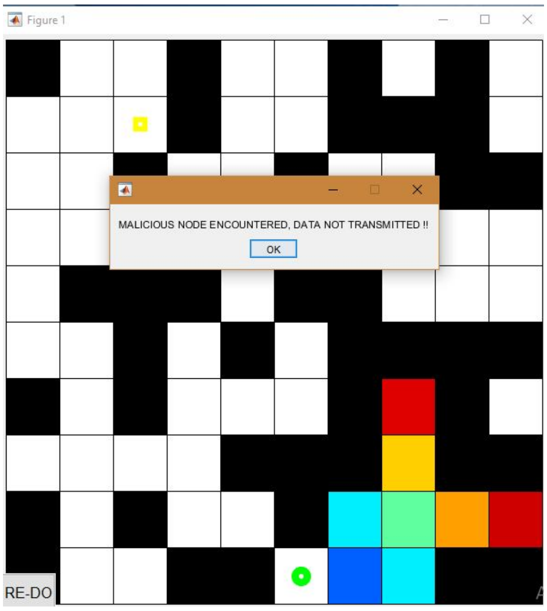


Fig. 5: CASE-I → Solution found and data transmitted successfully again.

In both figures from CASE-I the path is clearly visible that was chosen to transmit the packet from source node to goal node, obtained by tracing back from the goal node to the source node when no malicious node was triggered and data transmitted successfully.

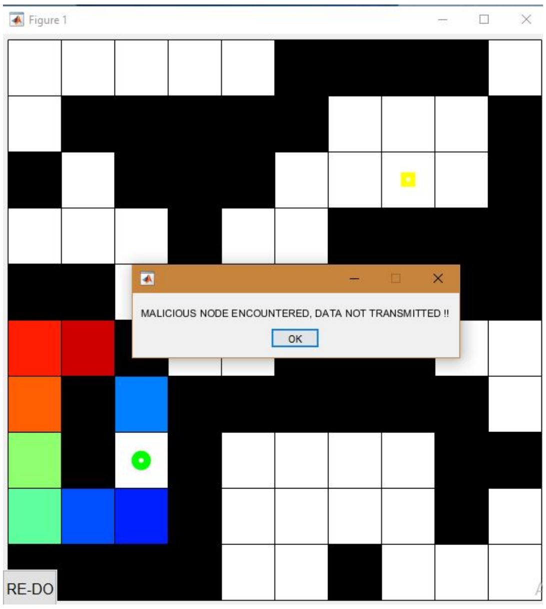


MALICIOUS NODE ENCOUNTERED, DATA NOT TRANSMITTED !!

OK

Fig. 6: CASE-II → Solution not found and data not transmitted.

In the CASE-II when the malicious node has been found in between the computed optimal path, a message box will pop-out be showing that malicious node encountered and data not transmitted.



MALICIOUS NODE ENCOUNTERED, DATA NOT TRANSMITTED !!

Fig. 7: CASE-II → Solution not found and data not transmitted again.

in the following manner we can conclude whether the malicious node is the result of the occurrence of the black-hole attack or grey-hole attack. If the malicious node appears in the very initial stage of data transmission then it shows the occurrence of the black-hole attack and if the data transmits successfully initially and then after sometime a malicious node occurred, it shows the occurrence of the grey-hole attack.

The code developed shows the 97% accuracy in the detection of a malicious node and is 99% accurate in rolling back the data packet to prevent it from transmission through the malicious node (attack). The remaining accuracy is lacking behind due to the reason of randomly selected nodes in the network matrix where the source node and goal node can be next to each other in position.

Although comparatively this approach is better than previous work done in the field of WSN security and prevention from threats. Since the code is simply implemented in MATLAB only, providing the practical solution for the threat detection and prevention.

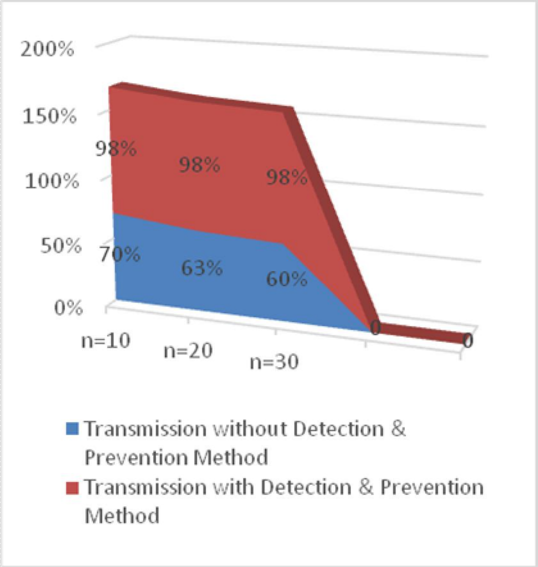


Fig. 8: Comparison Graph Plot

In the fig. 8 the comparison is between the WSN simulation between the data transmission with detection and prevention method and without this method, having varying number of sensor nodes, i.e. n=10, 20 and 30. In the WSN simulation the rates of successful data transmission were 70%, 63% and 60% respectively whereas after applying the method the rates were 98%, 98% and 98% respectively (97% accurate in detecting and 99% accurate in preventing, taking the average it becomes 98%).

VI. FUTURE WORK

We have successfully detected the malicious nodes and this approach can be used to securely detect the intrusion or malicious node and also then to prevent from the attack. In the coming future the work can be extended in various other direction as following:

- As we seen that if a malicious node is occurring again and again then this can lead to the situation of starvation where that data can never be transmitted successfully. So. there is a need of such a prevention method which could stop this from happening and let the data transmit.
- In this approach we are still unable to specify all different types of DoS attacks. Since, we are only indicating a particular node as a malicious node whether it is because of its anomaly or misuse or misbehavior or intruding activity. So, a better approach can be given to differentiate the type of malicious node to determine the attacks.
- ANN inspired from a human neural network NN [12], which can be used to make the IDS even more

powerful and efficient in the process of analyzing and decision making and to obtain a stronger and smarter IDS with prevention techniques.

VII. CONCLUSION

The main purpose of this research paper is to develop an IDS to successfully detect the intrusion and prevent the WSN from it. The developed code work shown above is successful in detecting the malicious node and then preventing the data packet from that malicious node by halting the data transmission. We have defined such system using the MATLAB only.

We developed a code in which a variable n*n size of matrix is considered to stimulate the WSN including all the 'n' number of sensor nodes. The optimal cost path is computed by traversing all the nodes between the source node and goal node which are randomly selected and then if the malicious node occurs the transmission stops and packet returns to the source node notifying about the solution being not found and malicious node being encountered resulting data not transmitted and otherwise the data transmits successfully to the goal node resulting the visible outcome of the path generated for transmission. In this approach the goal node and source node are selected randomly every time to stimulate the different cases. The number of nodes also can be changed and varied.

REFERENCES

[1] O. Can and O. Sahingoz,"A survey of intrusion detection systems in wireless sensor networks," in 6th International Conference On Modeling, Simulation And Applied Optimization, May 2015, p. Accepted.

[2] A.D. Wood and J.A. Stankovic, "Denial of service in sensor networks", IEEE Computer,Vol. 35, No. 10, pp 54-62,2002.

[3] I.F. Akyildiz, W. Su, Y. Sankarasubrananiam ,and E.Cayirci ,"A survey on sensor networks",IEEE Communication Magazine ,Vol.40 ,No.8, pp 102-114 , August 2002.

[4] W. Znaidi, M. Minier and J. P. Babau, "An Ontology for Attacks in Wireless Sensor Networks," Institute National de Recherche en Informatique et en Automatique, October 2008.

[5] M.A.Rassam,M.A.Maarof,andA.Zainal,"Asurvey of intrusion detection schemes in wireless sensor networks," American Journal of Applied Sciences,vol.9,no.10,pp. 1636-1652, 2012.

[6] J. P. Walters, Z. Q. Lian, W. S. Shi et al., "Wireless sensor network security: a survey," inSecurity in Distributed, Grid, Mobile, and Pervasive Computing, Auerbach Publications, Boca Raton, Fla, USA, 2006.

[7] D.W. Carman, P.S. Krus, and B.J. Matt, "Constraints and approaches for distributed sensor network security", Technical Report 00-010, NAI Labs, Network Associates Inc., Glenwood, MD, 2000.

[8] R.L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, Vol. 26, No. 1, pp. 96-99, 1983.

[9] G.Wang,J.Hao,J.Mab,andL.Huang,"Anewapproachto intrusion detection using Artificial Neural Networks and fuzzy clustering,"Expert Systems with Applications,vol.37,no.9,pp. 6225–6232, 2010.

[10] A. Abid, A. Kachouri, and A. Mahfoudhi, "Anomaly detection in WSN: critical study with new vision," in Proceedings of the International Conference on Automation, Control, Engineering and Computer Science (ACECS '14),pp.37–46,2014.

[11] N. A. Alrajeh, S. Khan, and B. Shams, "Intrusion detection systems in wireless sensor networks: a review," International Journal of Distributed Sensor Networks, vol.9, no.5,pp.1–7,2013.

[12] J.-S. Leu, T.-H. Chiang, M.-C. Yu, and K.-W. Su, "Energy efficient clustering scheme for prolonging the lifetime of wireless sensor network with isolated nodes," IEEE Commun. Lett., vol. 19, no. 2, pp. 259–262, 2015.