Sensor Validation Schemes: Contemporary Affirmation of the Recent Literature

Abdo M.T. Nasser
School of Computational Science
SRTM University, Nanded
Maharashtra, India

V.P. Pawar
School of Computational Science
SRTM University, Nanded
Maharashtra, India

ABSTRACT
Sensors are currently used in a lot of application areas such as health related application, military application, control and tracking application and habitat monitoring and environment applications. This paper introduces various number of sensor validation schemes in sensor network as an overview in this area. This paper entitles the description of the types of attacks and statement of the motivation for sensor validation in sensor network. Then, it introduces challenges of developing a typical sensor validation scheme for sensor networks which is followed by the major principle requirements of a good candidate sensor validation schemes. State-of-art of sensor validation schemes provided in this paper based on the techniques used in each schemes. Four major techniques of sensor validation are categorized as follows: Data mining, computational intelligence-based, rule-based, statistical-based and game theoretical based. Each schemes in this category is analyzed, showing their advantages and disadvantages. Finally, the survey concludes with presenting recommendations that provide some importance research opportunities in this area for future researcher.

Keywords
Data mining, computational intelligence (CI), rule-based.

1. INTRODUCTION
With the increase of the use of sensors in every day military and civil "common life activities", humans are replaced by sensors in certain mission which are too monotonous and too risky. Inspire of that, this complicated and very expensive machine are inevitable to false which main cause the mission failure or subject the system itself to dangerous or it is environment. For example, UAV (unmanned aerial vehicle) can crash because of fault.

The faults are not limited only to hardware tear and wear. A sensor should first sense the every altering dynamic environment and compute. it is believed over the world before it attempts to activate some actuators. This mix is important to select how behave and send the command to the related controller to activate the actuators. On the basis of its action, the world alters. Therefore, the mission operation goes ahead raptly. For instance, a sensors laser distance sensor returns a reading, which derives a belief of the distance to the target object. A movement towards the target objects it may be decided in the decisions making process of the sensor. This decision is interpreted to the execution of a cluster of command from a sensors APR. Every command activates some actuators as the sensors wheel. When the sensor is getting nearer to the target, the sensor react accordingly and the belief is updated. In every step of this seize, a fault may take place either owing to wrong false sensing or runtime errors or owing to a hardware failure.

This false should be detected and diagnosed quickly. For instance, when the code which computes the distance to the target crashes, the sensors may proceed to move forever. Constant value is deviated from the target or when the wheels are spinning in place. A survey on the nature of faults of autonomous sensor systems was conducted by Steinbauer et al [1]. Steinbauer et al come to the conclusion that the internal sensors are daily affected by faults to connectors or communication. They are crucial to task success. These faults are categorized as platform faults. Moreover, sensors are most affected by configuration problems. This sensor faults possess similar frequency but higher passive effect than platform false. Model-based approach is proposed for the function of detection and the diagnoses of sensor faults. This model-based approach relates sensor to internal hardware element in order to enable diagnose of this platform relevant false.

Sensor validation methods are survived in this paper. Therefore, four major techniques of sensor validation are categorized as follows: Data mining and computational intelligence-based, rule-based, statistical-based and game theoretical based. Each schemes in this categorize is analyzed, showing their advantages and disadvantages. Those Sensor validation schemes are provided in this paper based on the techniques used in each schemes.

2. CONTEMPORARY AFFIRMATION OF THE SENSOR VALIDATION SCHEMES
Neighbor-based sensor validation:
Sensor validation architecture is presented by Stetsko et al [2]. Propose sensor validation architecture on the basis of collaboration between neighbors. There are three types of attack for which they evaluated their schemes: Hello flood, jamming attacks and selective forwarding. Their scheme was executed for collaboration of Tree protocol (CTP) TinyOS environment. Even though the collaboration between nodes makes these schemes robust, the communication is problem. Moreover, high false alarm for detecting attacks is caused by the constructed rules like packet sending rate and packet dropping late. Another shortcoming of this study is that the power consummation rate related to the performance is not taken into consideration. This is a very crucial issue in sensor networks.

A new collaborative approach for sensor validation:
Lemos et al [3] have proposed a collaborative sensor validation scheme to detect node iteration attacks. This scheme is made on the basis of identifying some nodes to be monitor nodes for monitoring the conduct of other nodes in the network on the basis of satisfying group of predefine groups. They are fit for a certain attack type. There are special nodes called supervision nodes which, in turn, monitor the monitor nodes and are in charge of correlating the evidences

resulted by monitor nodes.In spite of the fact, this scheme looks strong in protecting the network by using two layers of protection. There are some shortcomings which restrict the utility of this scheme. In the beginning the supervisor nodes could constitute sources of failure when they have been compromised. There is another shortcoming related to the generality that is a main problem for the most rule-based schemes for sensor validation. Many suggestions have been made for the purpose of designing this scheme that is resulted from application.

Fuzzy logic sensor validation scheme for directed diffusion based sensor networks:A sensor validation scheme based on fuzzy logic is proposed by Chi and Cho [4]. There are some features of the traffic which were extracted to construct the fuzzy rules which are: node energy level, message transmission rate, neighbor nodes list and error rate in the transmission. The scheme was formed in order to prevent and detect from the denial of service attack that always drains the resource of the system. The base station or some monitoring nodes will be in charge of collecting the information messages from the neighbor. The fuzzy controller will calculate the detection value on the basis of the four features mentioned above.

It is noted that there is no clarity of how to select the neighbor nodes and the number of nodes that will be sufficient to protect the network. Moreover, there is a need for an expert or enough experience to make the rule ready and these results in the adaptability of scheme to detect new emerging attack. Another shortcoming is that the selected monitor node can be a point of failure if it is being compromised itself. Fuzzy logic sensor validation scheme against sinkhole attacks in directed diffusion based sensor networks:

Moon and Cho [5]. Proposed another fuzzy logic based sensor validation approach which aims to detecting sinkhole attacks in directed diffusion based on sensor networks. There are two features related to the directed diffusion protocols which are used. They are reinforcement ratio that is considered proportion of the reinforcement messages which are transmitted in an area to the numbering of sensing events from the nodes. The radius can be defined as the number of hop counts between any two nodes in the area concerning the sinkhole attack. The reinforcement message traffic in the area will be more than the normal number, while the number of hop count will be smaller. These two features will be used by the fuzzy logic controller as input to produce its output that is detection value. The controller will sign alarm that a sinkhole attack has occurred in the area. If the result detection value is more than predefined security threshold before the calculation of the detection values, an expert should set the fuzzy rules.

Prior to the calculation of the detection value, the fuzzy rules should be determined by an expert as per the symptoms of the sinkhole attacks.Because the input values are not always sharp values, using logic provides flexibility of detection of sinkhole attacks. In spite of that, the major problem of any fuzzy based scheme is the need for manual setting schemes.

Sensor validation based on Traffic Analysis and Fuzzy Inference System in Sensor Networks:A sensor validation scheme was introduced by Ponomarchuk and Seo [6]. For sensor network, they are presented by making use of two major traffic characteristics: the packet reception rate and the packet inter-arrival time in a time window. After that they apply fuzzy inference to make decision whether on attack has occurred or not. However, these scheme needs the rule to be prepared before the detection process, because it is based on fuzzy logic. The dependence on the previews knowledge that is the rule mix those scheme impractical concerning continuous stream environment such sensor network. Moreover, the author did not identify specified attacks to be detected by this scheme.

Advantages of Rule-based Sensor Validation schemes for Sensor Networks:

1. Fast detection: this is the feature which implements the need for online detection when there is a continuous streaming of the data in some sensor networks applications, because there is no training involved in this schemes.
2. The computational complexity is not dealt with here, because the schemes use only simple rules for detecting attacks.
3. Higher detection accuracy: this feature relies on comparison with some pre-defined rules.

Shortcomings of rule-based sensor validation schemes for sensor network:

1. Detection generality: the scheme can't be generalized to detect other types of attack because this scheme relies on the rules which are prepared by experts for specific types of attack. This occurs because different attacks possess different symptoms which required different rule.
2. Collaborative voting: this voting technique may increase the communication overhead, depending on collaboration between neighbors that vote to decide about the happening of an attack.
3. Assumption: most of the schemes place many assumptions before the building of their detection agent. These assumptions make schemes applicable for different applications.
4. The absence of standardized of evolution matrices: it is clear that most of those schemes use different methods to assess the efficacy of the scheme.

Data mining and computational intelligence based schemes:

Data mining and Computational Intelligence (DM/CI) techniques have been used comprehensively in constructing intelligent sensor validation schemes in computer networks since they have the ability to detect unfamiliar attack which cannot be detected by using the traditional based scheme. It is concerning a different sensor network to employee the DM/CI techniques on the limited resources. So, they use such techniques for building sensor validation scheme that are still in the early stages. There are subsection survey of the DM/CI based on sensor validation schemes which are used to detect attacks in sensor networks.

Clustering-based Sensor validation for attacks in Sensor Networks:

A data mining-based sensor validation scheme for Sensor Networks is proposed by Loo et al [7]. Every node in this scheme uses the fixed with grouping algorithm to form the normal profile from the known traffic behavior. Later on, abnormal activates which are caused by attacks are detected by the use of this normal profile. This scheme consists of three major stages:

1. Feature selection stage: in this stage the most important features which characterized the network traffic have been selected.

2. Cluster formulation stage: in this stage the similarity between the data traffic points are measured by applying Euclidean distance metric. Then, the clusters are formed.
3. The cluster labeling stage: in this stage, the results clusters are labeled on in the normal cluster much more than that number in the abnormal one.

According to the authors, this scheme has many merits which are as follows:

1. This scheme has the ability to detect unknown attack because it is unsupervised.
2. This scheme has a number of features which used to build the normal profile. This makes it suitable for detecting different types of attacks.
3. The fixed width grouping algorithm decreases the number of parameters required for grouping. It requires only one pass through the traffic samples.

In spite of all this advantage, this scheme is not free from some shortcomings which make it unsuitable for the resource constrained sensor networks. Here the most important shortcomings of the scheme are mentioned bellow:

1. The scheme has the most important shortcoming which is that every node must perform its own sensor validation independently. Consequently, this will consume the nodes power faster because of clustering algorithm.
2. The scheme has another shortcoming which is that the fixed distance threshold of the fixed width grouping algorithm makes the scheme inflexible.

Detecting selective forwarding attacks in Sensor Networks using SVM:
A centralized sensor validation scheme is proposed by Kaplantzis et al [8]. In order to detect selective forwarding and black hole attacks on the basis of one class Supper Vector Machine (SVM) and sliding windows. 2D feature vector which are bandwidth and count hop for the classification is used in this scheme. This scheme is entirely centralized in such way. That feature selection, processing, and decision making are all done by the base station. It is argued by author that this scheme have the feature of being energy efficient since it is totally centralized and the sensor nodes is not involved in the detection process. In other words, this scheme has small number of features which make it very specific and cannot be generalized for different kinds of attack. This scheme is only designed to detect how types of attacks, even though the use of machine learning techniques gives the scheme the generality by training the normal profile. That is to say that the selection of the features is very significant in making the scheme general or in generalizing the scheme to different types of attack.

Sensor validation in sensor networks is based on multi agent refined grouping: Huai-Bin et al proposed a multi- agent sensor validation scheme [9]. In order to detect attacks in sensor networks in this scheme, the mechanism of detection differs for various functions as follows:

1. Cluster heads are in change of monitoring all common member nodes in the group.
2. The common member nodes are in charge of monitoring the header of the group.

There are four types of agents which are installed on each sensor nodes to corporate in the detection. Every one of these nodes will fulfill different operation of detection as per its rule either cluster head or common node. In this scheme there are two grouping algorithms which are used into stages

1. **The first stage:**
   In this stage Self-Organizing Map neural network (SOM) is adapted for roughly grouping. The applying of this algorithm results in the number of groups and the group centers which are supplied for the second stage.
2. **The second stage:**
   This stage involves the k-means grouping algorithm to refine the groups that is generated in the first stage. Both the monitoring of the group heads support the security process. Nerveless, communication between the nodes and their group heads increase the communication overhead. There is another significant shortcoming which is the use of two grouping algorithm SOM and K-means. This causes a very high computational overhead and, consequently, consumes the nodes power in short time.

Optimized sensor validation using Genetic Algorithm (GA):
Khanna et al present a scheme in order to speed up the detection accuracy and decreasing the wrong alarm by selecting the appropriate nodes that will host the detection agents. Genetic algorithm was used for the purpose of evaluating sensor nodes attributes and examining its ability to be the local monitoring node (LMN) that works as a trusted agent for base station and capable of security monitoring its neighbors. There are some attributes such as utilization data, packet statics, battery status, and quality of service. The node fitness is measured on the basis of this attribute. Consequently, the GA selects the node which is appropriate and needs all these requirements to be the LMN.

It is argued that, this scheme is very suitable to cooperate with any detection schemes in order to concern resources usage and cannot be used alone for the detection. This scheme has a main shortcoming which is the high computational complexity of using GA due to the convergence time required when the scale of sensor networks is growing up.

Ant-based sensor validation schemes for sensor networks:Sensor validation scheme inspired by the ant colony algorithm is proposed by Muraleedharan and Osadciw [10]. The purpose of this scheme is to use multiple and agency in parallel search algorithm to deploy pheromone values. These pheromone values are used to detect the attacks in the network.

Initially, some direct and indirect path among their neighbors is determining by the nodes in this model. When any path is detected by the ant, it communicates the feature of the path through pheromone balancing to other ants. Then, when there is any imbalance in pheromone values, there will be an alert to let the administrate knowledge about a possible attack. This kind of scheme has a major advantage which is the self-organizing principle. The organizing principle is based on the probabilistic behavior. However, this scheme has also some shortcoming such as the high communication overhead due to the congestion and the high storage consuming. And packets are sent by the source node to all nodes through all possible path which make congestion that lead to high power

consummation. Moreover, every node must store very large list of pheromone value that makes use of the restricted memory of sensors.Design and implementation of EAR algorithms for detecting routing attacks in Sensor Networks:

Juneja et al [11]. present a sensor validation scheme for routing attacks in Sensor Networks based on EAR algorithm. It is an extension to their ant based scheme proposed in (Juneja and Arora) [11]. This scheme is based on three factors which are the Energy, Age and Reliability of the ant. The ants are classified into two main types: forward ants and backward ants. The forward ants report the information of the nodes in the path from the source node to the destination node, whereas the backward ants make use of the collected information to update the routing tables of nodes on their path and analyze the collected information to detect attacks.

Every node in the network has a log table that contains the information about their remaining energy, age of ant, the ratio of sent and delivered packets. The job of backward ants is to test values related to the stored values of the node and compares them with a predefined threshold value to verify that the path is reliable. The authors claimed that different types of attacks that could be identified using this scheme include sinkhole, black hole and jamming attacks. It is clear that the main drawback of this scheme is the high power consumption because of the ant‘s processing in two directions at every node in the network. This also causes a high communication overhead and congestion. The store of the three statistics energy, age and reliability is not reasonable when the number of sensors is very high and the number of ant used is also high.

Advantages of DM/CI based sensor validation schemes in Sensor Networks:

1. Less communication overhead: since most of schemes are based on the hierarchical structure of the Sensor Networks.

2. Generality is guaranteed: since the normal profile is not based on specific traffic features.

3. Scalability is also guaranteed: because the normal profile depends on the data and not on the architecture.

Shortcomings of DM/CI based sensor validation schemes in Sensor Networks:

1. Slow detection: because the data mining techniques like clustering require learning the normal profile, they are slow and therefore are not satisfying the streaming feature of the Sensor Networks that requires a fast solution or real time solution.

2. High computational complexity: because they involve the use of some complex machine learning algorithms or some difficult clustering approaches.
3. High false alarms: because they build the normal profile for a data in a specific point of time and there is no quick update, the normal profile could be out of data.

Game theory based Sensor Validation schemes in Sensor Networks:
The essence of the interaction between the sensor validation agent and the attacker can be represented scientifically by a game between two players. In these games, different strategies can be used by the sensor validation agent in order to defend against the different strategies that attackers always use. In the following, some game theoretical based Sensor Validation schemes in WSN are presented.

Detecting network intrusions via sampling:
A game theoretic approach introduces a game theoretic framework for effective detection of network intrusions by developing a network packet sampling strategy. In this framework, the intruder will choose the paths that minimize the chances of detection, while packet sampling strategy is used to maximize the chances of detection by the network operator. The game theoretic problem is first formulated and then the sampling schemes are developed so that to be optimal with the game approaches without exceeding a given total sampling budget.

This framework is among the first attempts to tackle the problem of sensor validation using the game theory. The idea behind choosing the paths either from the intruder or the network operator leads to the common routing issues specifically in the routing protocols that are based on the shortest path to determine its way to the base station. This advantage would make this framework suitable for detecting some kinds of attacks in the routing layer that are based on the routing path information. However, this framework still needs extensive simulation experiments to prove its viability and effectiveness to detect attacks.

Sensor validation in sensor network:
A non-cooperative game approach: Agah et al [14]. Proposed a non-cooperative game framework for the defense of nodes in Sensor Networks. In this framework, three different schemes have been applied to find the most vulnerable node in Sensor Networks and protect it. In the first scheme, an attack-defense problem is approached as two players, non-zero, non-cooperative game between the attacker and the sensor network. The second scheme uses the Markov Decision Process (MDP) to find the most vulnerable sensor node whereas the third scheme applies node’s traffic as an intuitive metric to use it as an indicator for protecting the node. The authors claimed that the evaluation of their schemes reveals its effectiveness of successful defense against attacks.

This study needs an experimental investigation to prove the concepts of the three used schemes. Another limitation of this work is that the strategy on when the MDP should be applied and when the theoretic game framework should be used to gain high success detection is not determined.

Detection of denial-of-message attacks on sensor network broadcasts:
A detection scheme of Denial of Message (DoM) attacks in Sensor Networks is introduced by McCune et al [15]. This scheme is designed for the broadcasting protocols in which the messages are broadcasted to the nodes periodically. The scheme is based on the Secure Implicit Sampling (SIS) method that enables the broadcasting base station to detect the failure of nodes to receive its broadcast in a probabilistic manner. The idea behind the SIS is that it works by extracting the authenticated acknowledgments from an unpredictable and tunable subset of nodes per broadcast so that it will minimize the acknowledgment implosion on the base station. The game theoretic approach here is used to evaluate the SIS method in facing optimal attackers that try to maximize the number of nodes denying the broadcasting of network messages.

Although this scheme is opening the door for research in this important area and as shown in the study agrees well with the

simulation scenarios, it has many limitations. The assumption that the nodes are always stable and immobile adds unrealistic constraints to the application of sensor networks for some critical environments. Another unrealistic assumption is that the node does not fail over time and this is not always true since there are many other reasons that may cause the failure of a node at any time.

The main advantage of this model is the use of the dynamic learning methods with the lack of information. This feature enables the players to consider the future costs for optimizing their strategies by the continuous learning about the potential attacks. However, this model needs to be evaluated by simulation experiments in order to validate the effectiveness of the Markov based sensor validation rather than the numerical analysis used in the evaluation.

Game theory model for selective forward attacks in Sensor Networks:

A framework using Zero-Sum game approach and selective node acknowledgements in the forward data path is proposed by Reddy and Srivathsan to detect selective forwarding attacks in Sensor Networks [16]. The authors provide mathematical foundations for detecting malicious nodes using selected points in the forward data path. They proved that selective acknowledgements are very useful to detect the malicious nodes through simulations. However, like other game theoretical approaches, this framework need to be more investigated experimentally to prove its concept.

Advantages of game theory based sensor validation schemes in Sensor Networks:

1. The game theoretical based sensor validation schemes do not need extra data to build the model and rather benefit from the routing information of the network.
2. The techniques used in these kinds of schemes are lightweight since no training is involved and are depending on some strategies.

Shortcomings of game theory based sensor validation schemes in WS:

1. It is obvious from the reviewed schemes that these schemes still concepts that need to be experimented extensively to prove their viability.
2. The scope of the game theoretical based schemes is limited to some layers information like the routing and application layers information because it builds the strategies based on some information from the network layer and application layers.

Statistical based Sensor Validation schemes in Sensor Networks:

The use of statistical techniques is common for anomaly detection schemes designed for Sensor Networks. These schemes use the probability distribution of either the normal or abnormal data as an evidence of attack behavior. The probability distribution model is first built and then compared to any deviation of data traffic generated later by the network. The following subsections describe some key statistical based Sensor Validation schemes used in Sensor Networks.

An anomaly detection algorithm for detecting attacks in Sensor Networks:Phuong et al present a new scheme based on the Cumulative Sum algorithm (Cu Sum) for detecting different kinds of attacks in Sensor Networks. This algorithm is one of the change point detection algorithm used to detect the change of the mean value of random sequence. In this scheme, the Cu Sum algorithm is employed to detect the changes in the number of incoming and outgoing packets as well as the number of collisions. A set of monitoring nodes is selected so that each sensor node is monitored by at least one monitor node.This scheme‘s main drawback is that the monitor node can be a point of failure easily since it is a normal sensor node. In addition, the implementation of such algorithm in a normal monitor node is power consuming.Group-based sensor validation system in wireless sensor network:

Li et al [9]. Propose a scheme in which the sensor network is partitioned into many groups using delta-grouping algorithm. In this algorithm, each group of sensors that are physically close to each other and has nearly the same sensing capabilities are grouped together. Some monitor nodes are chosen to monitor each group alternatively. After that a statistical distribution-based anomaly detection algorithm is used to detect the anomalies caused by attacks. According to the authors, this scheme takes into consideration multiple attributes of the sensor nodes in order to increase the accuracy of the detection.

The high computational complexity of the grouping algorithm and the statistical distribution algorithm are the main drawbacks since the common sensor node has limited resources. In addition, the monitoring node becomes a point of failure if compromised. However, this scheme has many advantages including the detection generality because of the use of several typical traffic features over the network.

Statistical wormhole detection in Sensor Networks:

Buttyan et al [17]. Proposed two mechanisms which are the Neighbor Number Test (NNT) and the All Distances Test (ADT) for detecting wormhole attacks in Sensor Networks. In the first mechanism NNT, the increase of the number of neighbors of the sensor is used as an indicator that new links have been created by the wormhole attack. In the second mechanism, ADT, the decrease of the lengths of the paths between the nodes is used as an indicator to the shortcut links created by the wormhole attacks. It is assumed that the sensor nodes send their neighbors information to the base station where the algorithm is applied on the reconstructed network graph by the received information.

Both mechanisms have been investigated by simulation and showed that they are effective in detecting wormhole attack with some limitations related to the radius of the area that is affected by the wormhole. The authors reported that high accuracy is achieved when the wormhole radius is comparable to the radius of the sensor radio range. However, these mechanisms only detect the presence of the wormhole attack but they do not provide any mean for localization of the affected area. Another drawback is related to the sending of neighbors’ information to the base stations by the sensor nodes and results in intensive communication overhead and consumes the power of the nodes on the way to the base station.

Malicious node detection in Sensor Networks using an Auto regression technique:

A strategy based on the past/present values generated by sensor nodes. In this study, the output of each sensor at each moment with its estimated value is computed to a predictor based on Auto Regression (AR) technique. If there is a big difference between the two values in any sensor, then this sensor becomes suspicious and an action should be done to mitigate its effects. The authors presented a case study to

prove the effectiveness of their concept with some assumptions that are set prior to the design of the AR technique. These assumptions are common in other Sensor Validation schemes for Sensor Networks but limit the applications of these schemes for different Sensor Networks applications.

Advantages of statistical based sensor validation schemes in Sensor Networks:
The statistical based schemes are mathematically proven and can be used effectively only if the accurate probability distribution model for normal or abnormal traffic is obtained.

Shortcomings of statistical based sensor validation schemes in Sensor Networks:

1. Usually the process of acquiring the correct probability distribution is not easy especially when no prior knowledge is available about sensor streaming data
2. Many of statistical schemes do not fit well with the multivariate data.
3. The dynamic streaming of network data makes it difficult to keep the probability distribution model up to date.

3. IMPORTANT FUTURE RESEARCH AREAS

In order to satisfy the requirements of an ideal sensor validation scheme, some important research opportunities open for further research:

1. Detection generality: to design Sensor Validation schemes that can be used to detect different types of attacks.
2. Detection speed: there is a need for a fast sensor validation scheme that satisfies the dynamic and continuous streaming of data in Sensor Networks.
3. The use of the lightweight Artificial Intelligence techniques: since these techniques have been used successfully for sensor validation in traditional networks, it is expected that their use here would enhance the anomaly sensor validation accuracy and generality.
4. The use of optimization techniques: these techniques could cooperate together with other techniques for choosing the best strategies of detection and the placement of detection agents
5. The integration between techniques from different categories: as proved their success in other domains, it would be interesting to try such integration. i.e., the rule-based and the DM/CI based schemes can be integrated together in such strategy of game theory to get the advantages of all of them.
6. Reducing the false alarm rates related to the DM/CI: since these schemes depend on the labeled data collected from the network, there is a high false alarm related to their application. It is interesting to look for solutions to mitigate this problem for the context of WSN.
7. Distribution of the sensor validation: because there is no single point in Sensor Networks, it can be used to install the sensor validation agent. And because the log data is collected in each sensor node, there is a need for a real distributed sensor validation scheme that can also minimize the power consumption results from the communication overhead with the base station in case of centralized sensor validation installation.
8. Unsupervised anomaly sensor validation: in fact, there is no labeled data set available for sensor validation in Sensor Networks. In addition, the design of such data set is not easy and costly task. It would be interesting to focus on the techniques, especially artificial intelligence and data mining techniques that do not require prior knowledge.

4. CONCLUSIONS

As the Sensor Networks becomes necessary and used frequently for many applications, the need for securing them is also increasing due to the nature of their deployment and their resource restrictions. Cryptographic and authentication protocols have been proposed to protect these networks from outsider intrusions but fail to protect them from the insider ones. Many surveys have been published for anomaly detection but according to the best of the researcher's knowledge none of them tackle the problem of sensor validation in specific. Instead, most of them focus on the anomaly detection in general assuming that the intrusion is kind of anomalies. In this article, it is surveyed about the Sensor Validation schemes in Sensor Networks. First, the paper states the fundamental issues of sensor validation in Sensor Networks showing the types of attacks, the motivation and the need for the sensor validation in WSN and the taxonomy of techniques used in the literature. After that, the challenges faced in developing an ideal sensor validation scheme were explored followed by the requirements for a good candidate sensor validation scheme. The classification of the-state-of-the-art Sensor Validation schemes proposed for Sensor Networks is then presented based on the technique used by each scheme.

The classification includes four main categories: rule based, data mining and computational intelligence based, game theoretical based and statistical based. For each category, an analysis has been carried out for each scheme highlighting their advantages and drawbacks. Finally, some important future research opportunities are pointed out for the future research.

5. REFERENCES

[1] G. Steinbauer. a survey on the nature of faults of autonomous robot systems. http://www.ist.tugraz.at/rfs/index.php/Main_Page

[2] Stetsko, A., L. Folkman and V. Matyas, 2010. Neighbor-based sensor validation for Sensor Networks. Proceedings of the 6th International Conference on Wireless and Mobile Communications (ICWMC), Sept. 20-25, IEEE Xplore Press, Valencia, pp: 420-425. DOI: 10.1109/ICWMC.2010.61 Tan, P.N., 2007. Introduction To Data Mining. 1st Edn., Pearson Education India, ISBN-10: 8131714721, pp: 792.

[3] Lemos, M.V.D.S., L.B. Leal and R.H. Filho, 2010. A new collaborative approach for intrusion detection system on wireless sensor networks. Novel Algorithms Techniques Telecommun. Netw.

[4] Chi, S.H. and T.H. Cho, 2006. Fuzzy Logic Anomaly Detection Scheme for Directed Diffusion Based Sensor Networks. Proceedings of the 3rd International Conference on Fuzzy Systems and

Knowledge Discovery, (FSKD' 26), SpringerVerlag Berlin, Heidelberg, pp: 725-734.

[5] Moon, S.Y. and T.H. Cho, 2009. Intrusion detection scheme against sinkhole attacks in directed diffusion based sensor networks. Int. J. Comput.Sci. Netw. Security, 9: 118-122.

[6] Ponomarchuk, Y.A. and Seo D.W., 2010. Intrusion detection based on traffic analysis and fuzzy inference system in wireless sensor networks. J. Convergence, 1: 35-42.

[7] Loo, C., M. Ng, C. Leckie and M. Palaniswami, 2006. Intrusion detection for routing attacks in sensor networks. Int. J. Distributed Sensor Netw., 2: 313-332.

[8] Kaplantzis, S., A. Shilton, N. Mani and Y.A. Sekercioglu, 2007. Detecting selective forwarding attacks in wireless sensor networks using support vector machines. Proceedings of the 3rd International Conference on Intelligent Sensors, Sensor Networks and Information Dec. 3-6, IEEE Xplore Press, Melbourne, Qld., pp: 335-340.

[9] Huai-Bin, W., Y. Zheng and W. Chun-Dong, 2009.Intrusion detection for wireless sensor networks based on multi-agent and refined clustering. Proceedings of the International Conference on Communications and Mobile Computing, WRI.

[10] Muraleedharan, R. and L.A. Osadciw, 2009. An intrusion detection framework for sensor networks using ant colony. Proceedings of the 43rd Asilomar Conference on Signals, Systems and Computers, IEEE Xplore Press, Pacific Grove, California, USA, pp: 275-278.

[11] Juneja, D. and N. Arora. 2010. An Ant based framework for preventing DDoS attack in wireless sensor networks. Int. J. Adv. Technol., 1: 1-11.

[12] Doumit, S.S. and D.P. Agrawal, 2003. Self-organized criticality and stochastic learning based intrusion detection system for wireless sensor networks.Proceedings of the Conference on IEEE Military Communications, Oct. 13-16

[13] Wang, S.S., K.Q. Yan, S.C. Wang and C.W. Liu, 2011.An Integrated Intrusion Detection System for Cluster-based Wireless Sensor Networks, Expert Syst. Appli., 38: 15234-15243.

[14] Agah, A., S.K. Das, K. Basu and M. Asadi, 2004. Intrusion detection in sensor networks: A noncooperative game approach. Proceedings of the 3rd IEEE International Symposium on Network Computing and Applications, 30 Aug.-1 Sept., IEEE Xpolore Press, pp: 343-346

[15] McCune, J.M., E. Shi, A. Perrig and M.K. Reiter, 2005.Detection of denial-of-message attacks on sensor network broadcasts. Proceedings of the IEEE Symposium on Security and Privacy, May 8-11, IEEE Xplore Press, pp: 64-78

[16] Reddy, Y.B. and S. Srivathsan, 2009. Game theory model for selective forward attacks in wireless sensor networks, Proceedings of the 17th Mediterranean Conference on Control and Automation, Jun. 24-26, IEEE Xplore Press,Thessaloniki, pp: 458-463.

[17] Buttyán, L., L. Dóra and I. Vajda, 2005. Statistical Wormhole Detection in Sensor Networks. In: Security and Privacy in Ad-hoc and Sensor Networks, Molva