ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 5, May 2018

An Integrated Intrusion Detection Model of Cluster-Based Visual Sensor Networks

[1] J.Beryl Tahpenes, [2] R.Nirmalan
[1] PG Scholar, [2] Assistant Professor, Department of Computer Science and Engineering, Sri Vidya College of Engineering & Technology, Virudhunagar

Abstract: **- Visual sensor networks (VSNs) are highly exposed to attacks since they are arranged openly in possibly solitary environments. Due to the bulky and bursty data traffic in VSN, it thrusts the need to establish mechanisms which provide reliable data communication across the network over the unreliable channels. Optimized Adaptive Boosting (OAB) algorithm is used for detection of anomalies in sensor nodes, cluster head nodes and Sink nodes. In this paper, in order to identify the modified packets or attacked packets at the receiver side, we propose a protocol named Efficient Secure Routing for Attacker Identification (ESRAI). This paper proposes an integrated intrusion detection model of cluster-based visual sensor network by combining anomaly and misuse detection, aiming at enhancing overall detection, security and System Accuracy. The proposed integrated model provides high throughput and more security, and it increases the efficiency of entire network when compared to the existing network.**

Key words: - VSN, Optimized Adaptive Boosting (OAB) algorithm, Cluster-based VSN, ESRAI protocol.

I. INTRODUCTION

Visual sensor network (VSN) is a network that consists of a large number of visual sensor nodes, which are capable of capturing multimedia data. With quick improvements in CMOS sensors, video coding techniques and embedded computing, VSNs have been widely used in traffic monitoring, habitat sensing and many other remote and video-based surveillance applications. Since the visual sensors of VSNs are usually deployed in unprotected or even militant environments, security is a matter of great concern. Hence the study on the security is obviously important. In recent years, many researches have put more emphasis on Security Routing, Encryption, Identity Authentication and other preventive systems for VSN security. Intrusion Detection could be classified into two: Anomaly and Misuse Detection. The aim of anomaly detection is to identify the data that exhibits abnormal patterns when compared with the patterns of the majority of data set. This detection is to classify the data as either anomaly (outlier) or normal. Misuse detection is to pick out any specific attack. So, an Intrusion Detection System is an effective improvement in the security of VSN.

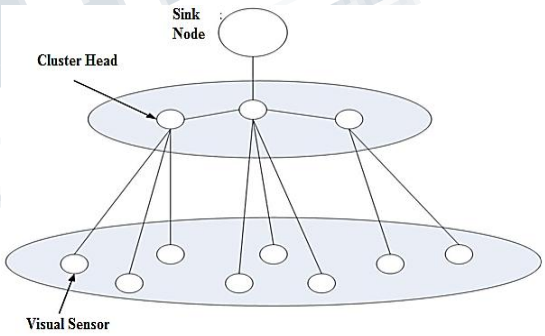


Fig:1 Cluster based VSN

II. LITERATURE SURVEY

Since Visual sensors could measure only the patterns, Reference [1] proposes a Traffic Pattern Learning method to sense the patterns captured by visual sensors. An active learning approach is also framed to better learn the pattern of attacks. It well addressed the Class Imbalance problem. However, it resulted in lesser overall detection of intrusions. To improve the detection rate, Reference [2] demonstrates a combined approach of the machine learning and misuse detection by using different types of classifiers such as Naïve Bayes, Multilayer Perceptron, J48 etc. to classify the attacks. As a result, accuracy rates get improved. Reference [3] proposes a preprocessing method of Adaboost for providing still

better accuracy for the classification of mislabeled data. It provides good generalization ability. Reference [4] proposes a q-gram distance for performing a search through the attack signatures to detect whether any attack present in the incoming traffic. This works well for the large number of combinations of distance computation parameters. Reference [5] proposes a hybrid intrusion detection system for security enhancement of cluster based WSN. In that, they outline the 8 common types of attack by using Back Propagation Network (BPN) with 99.81% detection rate, 99.75% accuracy and also avoids the resource wastage.. However when the training sample is unsubstantial, the individual detection rate was very low. Reference [6] proposes a improved IDS using fuzzy logic for intrusion detection. By using the data mining technique, the attribute selection process gets reduced. For faster decision making, they applied fuzzy interference engine using Mamdani interference mechanism with three variable inputs. However there occurs a bottleneck in packet processing. Thus it leads to slower intrusion detection. Reference [7] proposes an event driven VSN paradigm, which performs game theoretic analysis for the efficient handling of rich visual data. Reference [8] describes the design of a Short Life Artificial Fish Swarm Algorithm for activating the sleeping nodes with swarm intelligence. It also improves the coverage optimization approach, by short life behaviour, chasing behaviour and searching behaviour. It also provides a better convergence speed. But the network coverage changes according to the number of iterations. Reference [9] proposes a simultaneous Anomaly and Misuse intrusion detection approach based on the Set Theory with partial approximation. To discover the patterns within the data, they used a new data mining technique named Rough Set Theory. It enhances the partial-nature of security policies. Hence it is not possible to find accurately whether the system is secure or not. Reference [10] proposes a security protocol SPINS, Security Protocol for Sensor Networks, which consists of two building blocks comprises of two-party data authentication, data freshness evidence and confidentiality of data. µTESLA extends the broadcast in an authenticated manner for severely resource-required environments. These protocols are functional even with minimum hardware usage.

Considering the performance and the power of sensors, this paper proposes an integrated intrusion detection model of cluster based VSN. To enhance overall detection, security and system accuracy, this paper integrates the advantages of both anomaly and misuse detection. Optimized Adaptive Boosting algorithm is implemented in the process of detection of anomaly to construct a two-pass classifier. This could detect the anomalies in the cluster based VSN. In order to identify the modified or attacked packets at the destination, we propose a protocol named Efficient Secure Routing for Attacker Identification (ESRAI) protocol which generates misbehavior report automatically to intimate the status of received packets to source. Thus a misuse could be detected in the sink nodes of the cluster based VSN.

III. INTEGRATED INTRUSION DETECTION MODEL OF CLUSTER-BASED VSN

In this paper, proposed an integrated intrusion detection model for cluster based VSN. As shown in Fig 1, every cluster comprises of one Cluster Head (CH) and some visual sensor nodes. The Cluster Head has the responsibility to monitor the communications with visual sensor nodes. In each cluster, a large number of data transmissions between the visual sensor nodes are confined and also the long distance communications are restricted. This is to provide less complicated routing, higher efficiency. The Optimized Adaptive Boosting algorithm is proposed for detection of anomalies in sensor nodes, cluster head nodes and sink nodes, while the ESRAI protocol is for the detection of misuse in sink nodes.

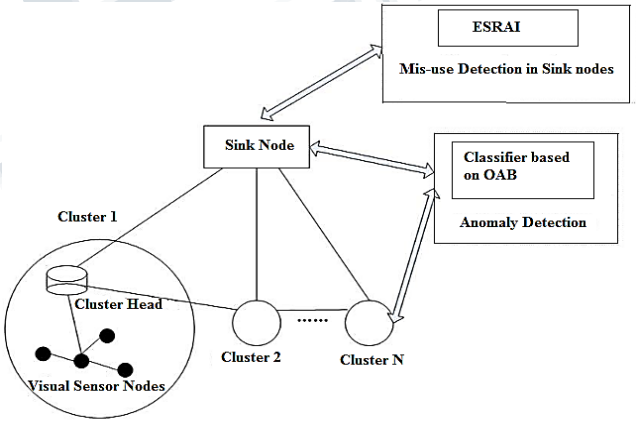


Fig: 2 Integrated Intrusion Detection model of cluster-based VSN.

3.1 ANOMALY DETECTION SYSTEM INSIDE CLUSTERS BY OPTIMIZED ADAPTIVE BOOSTING ALGORITHM

Due to the insufficient computing performance and low power of VSN, it consumes more time if stronger classifier is applied on visual sensor nodes. An Intrusion detection process requires fast and accurate responsiveness. To tackle this challenge, Optimized Adaptive Boosting algorithm is proposed for the detection of anomalies in cluster-based VSN. A strong,

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 5, May 2018

adaptable and highly stable classifier is constructed by integrating many weak classifiers. Hence it easily identifies the samples with negative features at preliminary levels and hence enhances the rate of detection and accuracy.

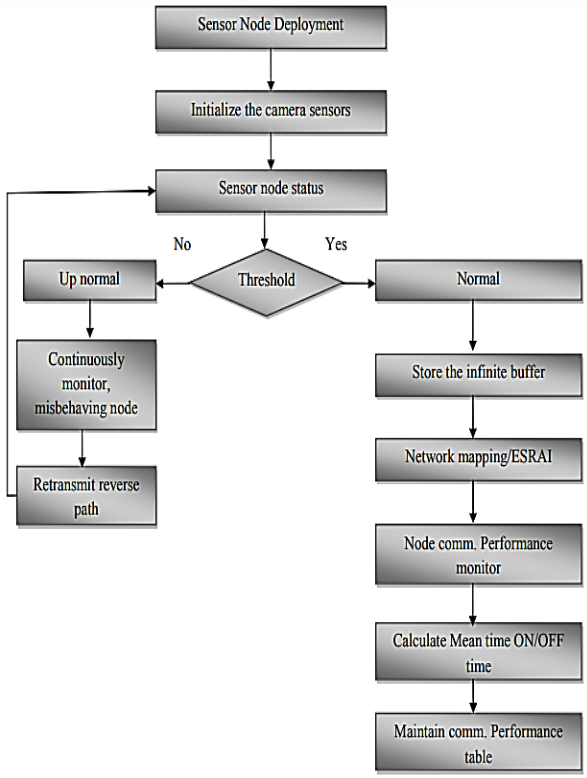


Fig: 3 Data flow in the Integrated IDS

The Fig: 3 depict the flow of data in the Integrated IDS. Well trained Optimized Adaptive Boosting is done in Sink nodes, Cluster Head nodes and Sensor nodes. In each level of classifier, if a data is fixed as normal one, it remains to be normal for all the succeeding levels. If it is determined as anomaly or outlier, detection process will be continued. The first level classifier at this level is accomplished with fewer preliminary features and with simple structure. Based on the given input, rate of detection will be high, at the same time some normal data may be concluded wrongly as anomalies. In the second level, as mentioned in Fig: 4, the i^{th} level classifiers work at Cluster Head nodes. Since it has a stronger computing capacity, it uses more complicated structures and with more features, Hence anomaly as like normal data can also be detected and the outcome from Cluster Head nodes is transferred to Sink nodes. At the sink nodes, the $(i+1)^{th}$ to nth level classifiers function, If data is determined as anomaly, it will be intimated to the controller and the node will be resettled and included in the network.

3.2OPTIMIZED ADAPTIVE BOOSTING ALGORITHM (OAB)

Optimized Adaptive Boosting Algorithm belongs to the category of classic algorithms in the data mining process. This algorithm works in an iterative manner. The main focus of this algorithm is to train various weak classifiers for the same training set, later on all these will be combined to form a stronger classifier. If the weight of the trained sample falls, then it would be correctly classified by the classifier. The selection probability will be smaller. If the weight of the trained sample rises, then the selection probability will be larger. Thus Optimized Adaboost algorithm concentrates more on the samples that can be easily misclassified. Thus the algorithm forms classifier which is strong enough to improve the rate of detection of anomalies.

Input: Select training set S = $\{(x_1, y_1),\ldots\ldots,(x_i, y_i)\}$, where $x_a \in X$, $y_b \in Y = \{-1,1\}$, 1 is Normal sample and -1 is Anomaly sample, a= 1,2,3,……,i;

T-Number of weak classifiers (Maximum number of iterations)

Output: Strong and stable classifier constructed from T weak classifiers

Begin

Initialization of sample's weight x_a

$$\begin{cases} \text{Normal sample } w_{t,m} = 1/2r \\ \text{Anomaly sample } w_{t,m} = 1/2s \text{'} \end{cases}$$

where r is the number of Normal samples and s is the number of Anomaly samples.

While not end

Do

Begin

For 1 to T, // train classifier h_t by T iterations and evaluate $h_t(x_a) \in \{-1,1\}$, Training error.

$\varepsilon_t = \sum_a w_{t,a} \, I\,(y_a \neq h_a(x_a))$

if(ε_t=0 || $\varepsilon_t \geq 0.5$)

break;

then

refresh $w_{t,a}$,

Proceed the successive training

$w_{t+1,a} = \frac{w_{t,a}}{z_t} \cdot e^{c_t y_t h_t(x_a)}$,

where Z_t is normalized coefficient,

$c_t = \frac{1}{2} \log \frac{1-\varepsilon_t}{\varepsilon_t}$

End For

End

Output: Strong and stable classifier

End function

$H(x) = \text{sgn}(\sum_{t=1}^{I} c_t \; h(x) - \theta)$

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 5, May 2018

Where sgn is the sign function.
Samples are classified in accordance to the value of H(x).
θ is end threshold value, and the average value of all the weak classifiers is the initial value.

$$\theta = \frac{1}{T}\sum_{t=1}^{T} c_t$$

End

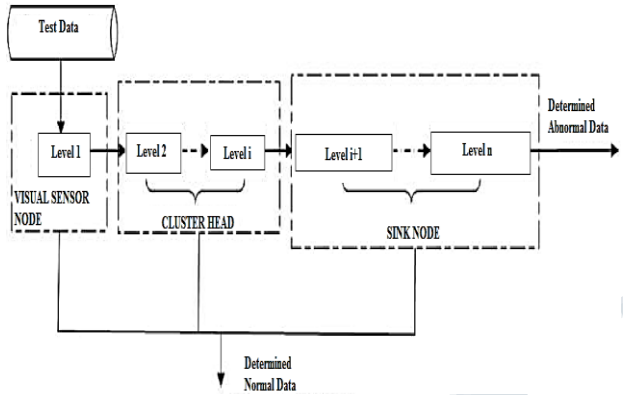


Fig: 4 Flow of Cluster based Anomaly Detection

3.3 MISUSE DETECTION OF SINK NODES BY ESRAI (EFFICIENT SECURE ROUTING FOR ATTACKER IDENTIFICATION)

In order to identify the modified or attacked packets at the destination we propose a protocol named Efficient Secure Routing for Attacker Identification (ESRAI) protocol that produces a misbehavior report automatically to intimate the details of received packets to the source. At the receiver side, to detect the correct packets, the threshold value of the transmitted node will be taken into account by ESRAI protocol. It checks the threshold value at the destination. If it is constant, then the receiver assumes that the received packet is original and produces an acknowledgement to the source. If the packets are viewed or modified by an attacker before reaching the destination, the threshold value will get altered and then it is identified as duplicate in the receiver side. Thus, ESRAI protocol produces a misbehavior report automatically to the source.

ESRAI PROTOCOL

Neighbour Nodes Collection ΔN_{ix}

Source Model Initialization ΔS_{ix}

Agent Attachment ΔR_{ax}

ID of Packet ΔP_{id}

Nodes Activity ΔN_{ix} in Packet Mode

$\Delta N_{ix} = \Delta P_{ckt}$

In Packet Mode Number of Packets 1200

For (ΔP_{id} = 0; ΔP_{id} < N; ΔP_{id} ++)

Begin

If P_{ckt} =A

P_{ckt} <= Attacker is injected

Send the Misbehaviour Report and S-ACK //Send Duplicate Report

Else

P_{ckt} = B;

P_{ckt} = Attacker is not injected

Send (ACK) the Acknowledgment Packet ID

End if

End Process

Destination ΔD_{ix}

$\Delta D_{ix} <= \Delta R_{ax} + \Delta S_{ix}$

The proposed protocol provides more secured transmission in the Cluster based Visual Sensor Networks. It is easy to identify the packets which are under attack and its corresponding attackers too. The ESRAI protocol can produce a misbehavior report automatically when it receives an attacked packet at the receiver side. Due to the proposed protocol, Overall Detection rate and Security of entire network is enhanced when comparing with the existing methods.

IV. RESULT

After the sample traffic is generated, we evaluated the performance of the proposed integrated IDS. Particularly, the weak classifiers are boosted with the Optimized Adaptive Boosting algorithm and the nodes are classified according to their respective threshold value. From this the anomalies were detected. Using the ESRAI (Efficient Secure Routing for Attacker Identification) misuse of several nodes was detected. Then we evaluated the rate of detection for different attacks, overall detection performance, the capability to detect new attacks, and also the real-time performance of the Intrusion Detection System. The evaluation measures applied to model the performance of IDS in detection process includes Overall Detection rate, System Accuracy, Security.

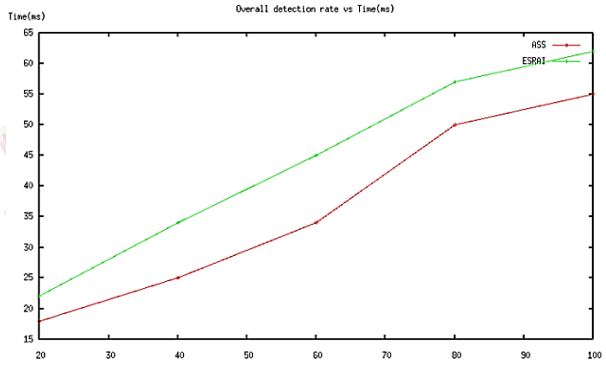
ISSN (Online) 2394-2320

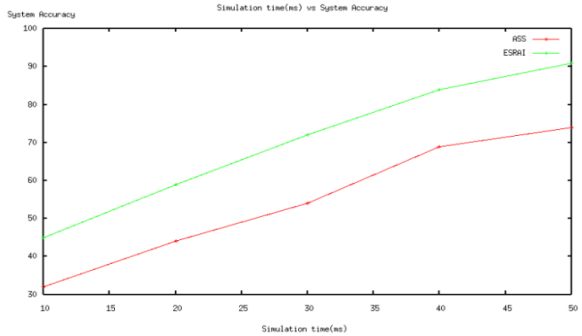
International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 5, May 2018

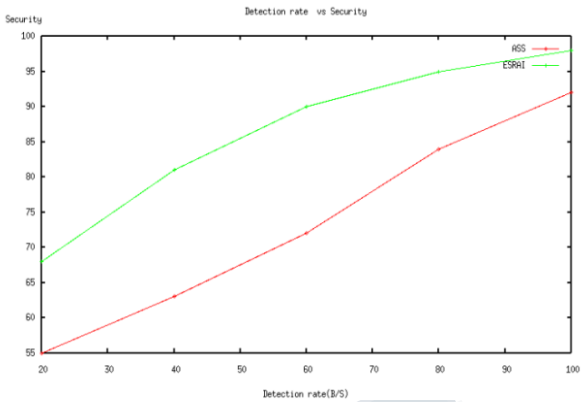
	Normal	U2R	DoS	R2L	Probe	Total
Anomaly Detection Training Set	3000				2000	5000
Anomaly Detection Test Set	2000				1000	3000
Misuse Detection Training Set	803	56	3137	239	765	5000
Misuse Detection Test Set	479	37	1880	152	454	3000

Table 1 Training and Test Samples Selection

In this paper, training data sets and test datasets used are from KDD CUP 99. In this analysis 5000 data are selected as training samples and 1000 data as test samples from the 10% KDD CUP 99 dataset was taken, as shown in Table 1. On comparing the proposed ESRAI (Efficient Secured Routing for Attacker Identification) protocol with the ASS (Attacker Identification using Segment Splitting), we achieved a better performance with the considered evaluation criterion. The Overall Detection rate of ESRAI increases with increase in time when compared with ASS. As the simulation time increases, the system provides better accuracy than ASS. ESRAI provides more security than the ASS scheme.







V. CONCLUSION

Providing security to the data under transmission within a cluster based wireless sensor network is a real challenge for network administrators. If there exists an intruder, the intrusion detection system should be able to detect the anomalies or misuse with a high rate of detection and low positive rate. The proposed Optimized Adaptive Boosting Algorithm is capable of detecting the anomalies which intrudes in the network. While the proposed ESRAI (Efficient Secure Routing for Attacker Identification) protocol helps to provide high security to the packets under the transmission and transmits a misbehavior report to the controller when there exists an attack. The proposed integrated model provides high accuracy and it increases the efficiency of entire with enhanced Overall Detection rate when compared to the traditional network. In future, we will take the energy level of nodes and the information entropy for VSN into account.

REFERENCE

1. Kaixing Huang, Qi Zhang, Naixue Xiong, Yuanquing Qin, "An Efficient Intrusion Detection Approach for Visual Sensor Networks based on Traffic Pattern Learning" in IEEE 2017.

2. Xiangyang Liu, Yaping Dai,Yan Zhang, Qiao Yuan, Linhui Zhao, "A Preprocessing method of Adaboost for Mislabeled Data Classification" in IEEE 2017.

3.Rohini Rajpal, Sanmeet Kaur, Ramandeep Kaur, "Improving Detection Rate using Misuse Detection and Machine Learning" in IEEE 2016.

4.Fei Lei, Lei Yao, Deng Zhao, Yucong Duan, "Energy efficient abnormal nodes detection and handlings in wireless sensor networks" in IEEE 2016.

5. V.Jaiganesh, S.Mangayarkarasi, Dr.P.Sumathi "Intrusion detection systems: A survey and analysis of classification techniques" in IJARCCE 2013.

6. Zoltan Csajbok "Simultaneous Anomaly and Misuse Intrusion Detections based on Partial Approximative Set Theory" in IEEE 2011.

7.K.Q.Yan, S.C.Wang, S.S.Wang, C.W,Liu "Hybrid Intrusion Detection System for Enhancing the security of a cluster-based Wireless Sensor Network" in IEEE 2010.

8. Bharanidharan, Shanmugam "Improved Intrusion Detection System using Fuzzy Logic for Detecting Anomaly and Misuse type of attacks" in IEEE 2009.

9. Ashfaq Hussain, Farooqi Farrukh, Aslam Khan "Intrusion Detection Systems for Wireless Sensor Networks: A Survey" in Springer 2009.

10. Wojciech, Tylman, "Misuse-Based Intrusion Detection Using Bayesian Networks" in IEEE 2008.

11.Alexandra Czarlinska, Deepa Kundur "Coordination and Selfishness in Attacks on Visual Sensor Networks" in IEEE 2008.

12. Ting Yang, Tang Young, "Short Life Artificial Fish Swarm Algorithm for Wireless Sensor Network" in IEEE 2013.

13. Slobodan Petrovic, Sverre Bakke, "Improving the Efficiency of Misuse Detection by Means of q-gram Distance" in IEEE 2016.

14.Adrian Perrig, Robert Szewczyk, J.D.Tygar, Victor Wen, David E.Culler "SPINS: Security Protocols for Sensor Networks" in IEEE 2002.

15. Peter Lichodzijewski, Malcolm, I.Heywood "Host-Based Intrusion Detection Using Self-Organizing Maps" in IEEE 2002.