*International Journal of Engineering & Technology*, *7 (1.1) (2018) 565-569*

**International Journal of Engineering & Technology**

*Website: www.sciencepubco.com/index.php/IJET*

***Research paper***

# Enhanced replica detection scheme for efficient analysis of intrusion detection in MANET

**P. Bakeyalakshmi [1], Dr. S. K. Mahendran [2] ***

*[1] Research Scholar, Department of Computer Science, Bharathiar University, Coimbatore, Tamilnadu, India*
*[2] Assistant Professor, Department of Computer Science, Government Arts and Science college, Udhagamandalam, Tamilnadu, India*
**Corresponding author E-mail: sk.mahendran@yahoo.co.in*

## Abstract

Nowadays, detection scheme of intrusion is placing a major role for efficient access and analysis in Mobile Ad-hoc network (MANET). In the past, the detection scheme of Intrusion was used to identify the efficiency of the network and in maximum systems it performs with huge rate of false alarm. In this paper, an Effective approach of the Enhanced Replica Detection scheme (ERDS) based on Sequential Probability Ratio Test (SPRT) is proposed to detect the malicious actions and to have a secure path without claim in an efficient manner. Also, provides strategies to avoid attacker and to provide secure communication. In order to have an efficient analysis of intrusion detection the proposed approach is implemented based on the anomaly. To achieve this, the detection scheme is established based on SPRT and demonstrated the performances of detection with less claim. The simulation results of control overhead, packet delivery ratio, efficient detection, energy consumption and average claims are carried out for the analysis of performance to show the improvement than the existing by using the network simulator tool. Also, the performance of the proposed system illustrated the detection of intrusion in the normal and attacker states of the network.

***Keywords***: *ERDS; Detection Scheme; MANET; Detection Efficiency; Delay; Network Lifetime.*

## 1. Introduction

Nowadays, in many applications the unstructured network of Mobile Ad-hoc Network (MANET) became a major role and provides an efficient communication process in an efficient manner. In the network each node is considered separately and the decision making is carried out by the node itself. Therefore, there is no central management in the network between nodes. In order to manage the nodes intrusion detection approach is developed and it is classified into signature and anomaly based intrusion detection.

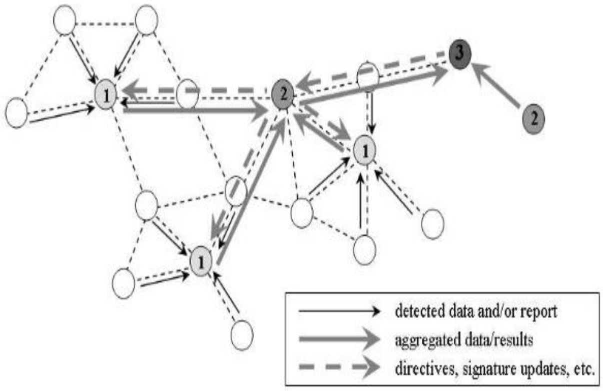

1
2
3
2
1
1
detected data and/or report
aggregated data/results
directives, signature updates, etc.

**Fig. 1:** Dynamic Intrusion Detection.

Basically the Intrusion detection system (IDS) is a challenging task due to the MANET dynamic nature. Fig [1] shows the dynamic IDS hierarchy. The signature based detection scheme is used to find the matches and attack pattern between the network traffic. As well as the anomaly based scheme is used to develop the profile according to the normal network behavior. By this scheme the detection is considered inbuilt and the network is monitored. As per the learning of behavior the detection and monitoring is carried out without any prior knowledge regarding the network.

The detection of intrusion is based on the anomaly in this work. Here the process of communication is carried out in an efficient manner with the improvement of claims and avoidances of attack. The packet transmission is resolute with the network monitoring and it is based on the profile created. The detection of intrusion can process at any state and it is derived as per the procedure of the scheme. Also, the network traffic is considered and simulated. The intention is analyzed based on the parameters and strategies.

The framework of detection scheme is performed in an adaptive manner. It ensures the secure communication and robustness of the system in terms of improvement in average claims, energy consumption, control strategies and latency. The process of IDS is done in a secure module of communication based on the agent as shown in Fig [2]. In this paper, the detection scheme is done by implementing the proposed approach of SPRT based ERDS for the reduction of claims and avoidances of attack with better performance.

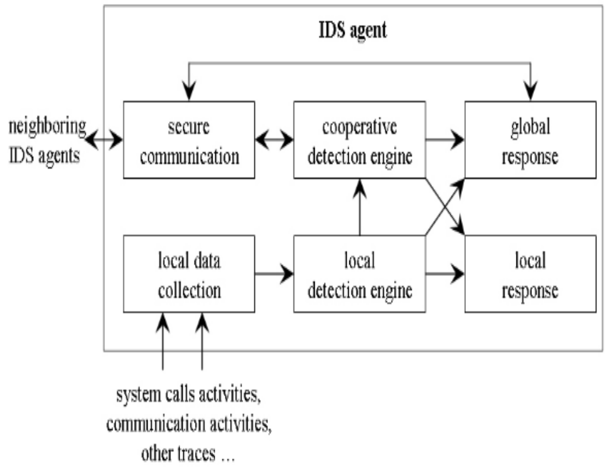


**Fig. 2:** IDS Agent Model.

The rest of the paper is arranged in section wise. In section 2, the survey of IDS and its related approach is discussed. The proposed approach explanation and implementation are carried out in section 3 and the simulation results analysis of performance is in section 4. Finally, the conclusion is available in section 5.

## 2. Related work

In this section, the literature survey of the intrusion detection in the network and its approach is discussed. In detection scheme trust based approach is implemented for secure process. Here the performances of the network with the packet transmitting, drooping rate and the correlation between packet losses are considering. It provides an efficient process by using a public auditing architecture based on homomorphic linear authenticator (HLA). It reports the loss of packets and verify the information is truthful or not [1].

A new intrusion-detection system of Reinforce Adaptive ACKnowledgment (RAACK) is especially considered for MANETs. The malicious attackers make the report of false positive and innocent nodes of falsely report as malicious. This attack can be terminated when the sufficient nodes break down by the attacker to the entire network and thus cause the division of the network. The IDS was accomplished by identifying malicious nodes despite the reality of false report of misbehavior [2].

The proposed lightweight and energy-efficient system is used for the detection of intrusion in intrusion based on the metric of the sensor node energy consumption. A linear regression model was function to predict the consumption of energy. The results indicated the high accuracy, while having very low false-positives [3].

The developed intrusion detection algorithm is considered using t-distribution and the robust model is processed the sensor nodes of multiple attributes. This model exploited the approximate parameter to detect malicious attackers accurately. It achieved accurate detection and low false alarm rate even few nodes misbehaving, and quickly perform with a lower computational cost [4].

The proposed trust-based systems establish the distributed system with ensuring the security. The trust-based approach creates WSNs tolerant besides the targeting of routing layer by attacks. It provides a low overhead when compare to the system of unprotected [5].

The $K$-nearest neighbor classification approach based IDS is considered for separating the normal nodes from abnormal by observed behavior of abnormal nodes. The analysis of the system is as per the parameter selection and IDS error rate. It achieved improved and efficient detection by improving the protocol of distance vector routing [6].

For the avoidance of network the DSA and RSA is implemented with the scheme of IDS. Furthermore, in the communication, both sending and receiving nodes are not malicious. Unless identified, all packet responses described to be digitally signed by its sender and receiver verifies it [7].

The misbehavior detection is based on the system features and it is performed by using genetic and set theory approach. The data on cross layer it characterize the mobile nodes behavior. It improved the overhead reduction and increases the detection accuracy [8].

Enhanced Adaptive Acknowledgement is developed for the avoidance of malicious attacks. The packet forwarding of reliable neighbor nodes is not considered and the neighbor's recommendation is used for route discover and management [9]. The trust and reputation based IDS design is used for decision making and analysis of malicious attacks with possible sources [10].

A feature selection methodology is developed for the data analysis. The features are tested under various operating condition and analyze the features selected. The irrelevant and redundant often maximize the system performance and it occurs in the accuracy of prediction and speed. By using principal component the analysis and the selection of features is carried out. It analyzed various trials for the state simulation of normal and attack [11].

The IDS scheme has developed with the approach of clustering to build the normal traffic behavior model. It detects the abnormal patterns and its process set of features which applied to a wide range of routing attacks [12].

The detection of routing attacks is done by using the IDS and the framework of mathematical. This framework is carried out the with the Byzantine attackers performance. In order to have an efficient process game theory based the framework is developed [13].

## 3. Proposed approach

In this section, the proposed approach explanation and the implementation are presented. The proposed approach of the Enhanced Replica Detection scheme (ERDS) based on Sequential Probability Ratio Test (SPRT) is considered to provide less average claims, efficient detection and better performance of energy consumption, end to end latency, control overhead and packet delivery ratio. The analysis of the nodes is performed throughout the network and considers the limitation with the maximum speed of a system configured. Here, the node communication is in bidirectional through the link of communication. All the node's clocks are synchronized loosely and communicate with a base station. The station may be reliable on the basis of regular.

The statistical process of decision making in the network is considered randomly with the limits of lower and upper. The hypotheses process is defined the associated towards the lower and upper limits with every observation. The selection process is considered according to the limit and proceeds with the selection or termination or null, respectively. As well as configured with the maximum speed as per the limits it considered.

However, the network is analyzed it is done by using the Sequential Probability Ratio Test (SPRT). It processes every node's neighbor with the claim and its details of time, location and speed. However, the decision computes the speed as per the sample observed and the limits and leads to the replication and alternate acceptation of the base station. If it replicated the nodes, then it revokes the network replica node.

a) Claim Generation and Forwarding

The nodes travel to the new location each time and it discover the nodes location and collection of neighbor nodes. Each node needed the authenticated claim location by passing the current time and it checks the received time is valid or not.

$$|T' - T| > \delta + \in \tag{1}$$

Where, $T'$ is defined the time receipt of claim, δ define the claim delay of transmission and ∈ represent the synchronization time of maximum error. Each claim generated with the private key by RSA approach for process and if it consists invalid time, then the claim will fails to authorize and remove the node. Also, the range of the signal is higher for the distance or location of the claims.

After filtering the unauthorized nodes the nodes are forwarded the claims with probability to the base station.

b) Detection and Revocation

The claim of location from node is processed based on the public key using the RSA approach and the verification of claim authentication by the base station. The process is carried out with the encoding and decoding process using RSA approach. The distance and the speed are estimated using Euclidean distance and all the parameters are defined to have average claim and better performance.

As per the ratio of log probability the SPRT is carried out as given below.

$$l_n(\beta' / (1-\alpha')) < l_n((1-\beta') / \alpha') \tag{2}$$

c) Enhanced Replica Detection Scheme

In the network the transmission of packets is considered between the sender and the nearest nodes with the acknowledgement. The process of route path is discovered the transmission between nodes.

```
Algorithm: SPRT based Enhanced Replica Detection
Begin
Initialization of parameters
If x>o then
Compute time (T) and speed;
If 0>$V_{max}$ then
$\omega_x = \omega_x + 1$;
end if
if T(x)<= $\omega_x$ then
Accept hypothesis and test terminate;
end if
if T(x)>= $\omega_x$ then
Initialize zero and accept hypothesis;
return;
end if
end if
x=x+1
p-loc=c-loc;
p-time=c-time;
```

As per the request and response of the route, the sending and receiving of a packet is carried out. If there is any interrupt the process is stop the forwarding and send the message regarding the issues. The metric of energy, leaving the node, bandwidth and the joining node are considered for the transmission of packets.

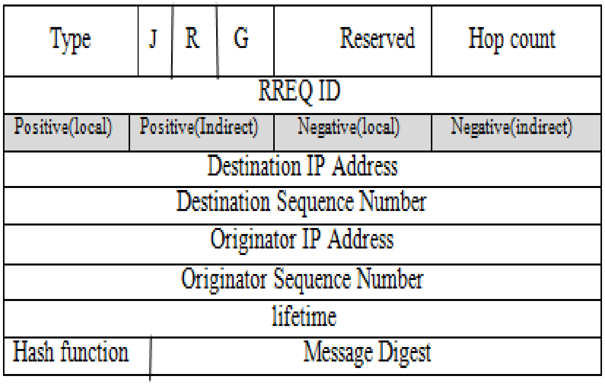
As per the metrics the detection procedure is performed for each node. The negative point is defined if the energy is lower than the threshold and also the bandwidth is compared with it. As per the request of the node and the process the negative values are applied to the abnormal nodes. During the communication if any of the node authority is failed, then the node is replicated. The authentication is based on the approach of RSA. According to flow the replica detection is carried out in the network.

The limitation of attack replica node is determined when the approach is employed. The accuracy of detection is estimated by the error probability of false positive and false negative and it is based on the limits of upper and lower. Also, it is process according to the SPRT.

$$\alpha' + \beta' \geq \alpha + \beta \tag{3}$$

d) Packet Format

As given in the below packet format the proposed system is implementation is carried out.



<table>
<tr><td>Type</td><td>J</td><td>R</td><td>G</td><td>Reserved</td><td>Hop count</td></tr>
<tr><td colspan="6">RREQ ID</td></tr>
<tr><td>Positive(local)</td><td colspan="2">Positive(Indirect)</td><td colspan="2">Negative(local)</td><td>Negative(indirect)</td></tr>
<tr><td colspan="6">Destination IP Address</td></tr>
<tr><td colspan="6">Destination Sequence Number</td></tr>
<tr><td colspan="6">Originator IP Address</td></tr>
<tr><td colspan="6">Originator Sequence Number</td></tr>
<tr><td colspan="6">lifetime</td></tr>
<tr><td>Hash function</td><td colspan="5">Message Digest</td></tr>
</table>

## 4. Simulation results

In this section, the simulation of the proposed system is simulated using the network simulator tool (NS2) and the performance analysis is carried out with the comparison of results. In this work, the results comparison of the proposed approach is done with the attack like a black hole and Sybil.

As well as, the approach is compared with the values (values are 0.01 and 0.1) of true positive and true negative for the estimation of average number of claims in the network. The parameter setting of the proposed system is given in Table [1].

**Table 1:** Parameter Settings

| PARAMETERS | VALUES |
|---|---|
| Simulator | NS-2.34 |
| Simulation area | 1400m x 1200m |
| No. of nodes | 50 |
| Simulation time | 50s |
| MAC type | IEEE 802.11 |
| Traffic type | CBR |
| Mobility model | Random |
| Mobility speed | 5 m/s |
| Protocol | AODV, DSDV and DSR |
| Transmission Range | 150 m |
| Initial Energy | 100 joule |
| Frequency | 9 Mhz |

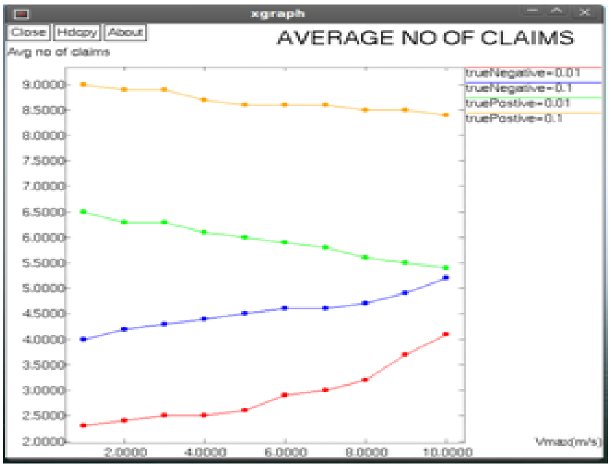


**Fig. 3:** Performance Analysis of the Average Number of Claims.

Fig [3] shows the analysis of the proposed approach average number of claims on the network with true positive and negative. Fig [4] shows the analysis of claims with the comparison positive true values only.

Fig [5] shows the analysis of control overhead of the proposed approach. Here the analysis is considered between the attack that determines the performance of the proposed approach in both attacks of Black hole and Sybil. It is carried out for the analysis.

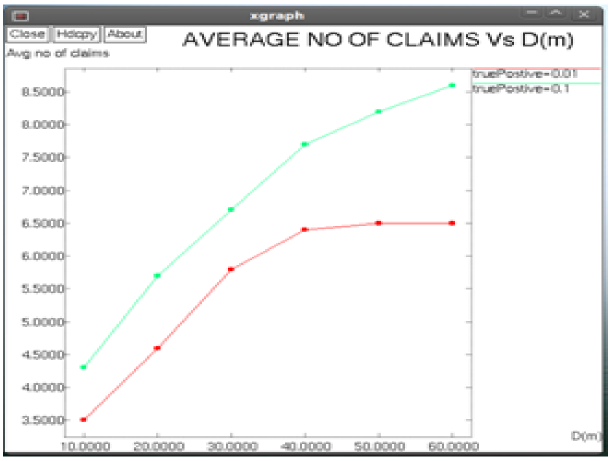


**Fig. 4:** Performance Analysis of Average Number of Claims Vs Distance (M).

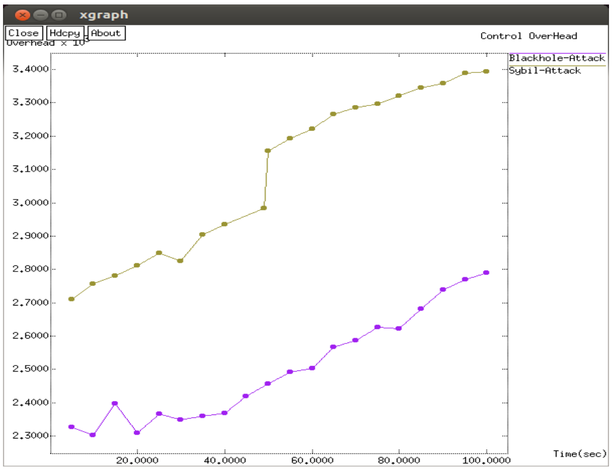


**Fig. 5:** Performance Analysis of Control Overhead.

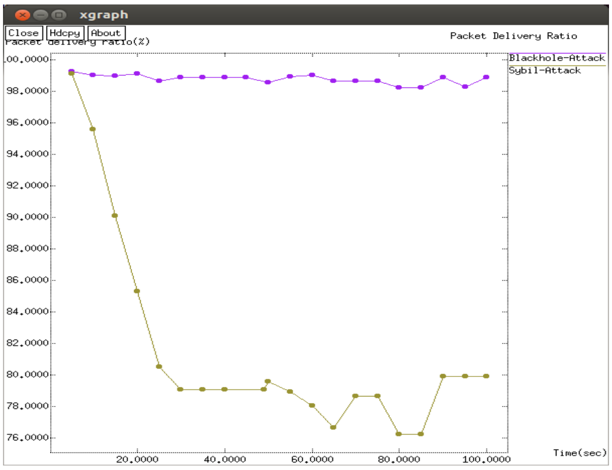


**Fig. 6:** Performance Analysis of Packet Delivery Ratio.

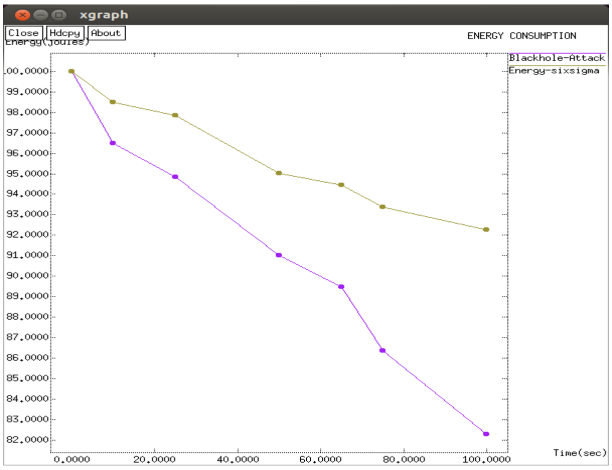


**Fig. 7:** Performance Analysis of Control Overhead.

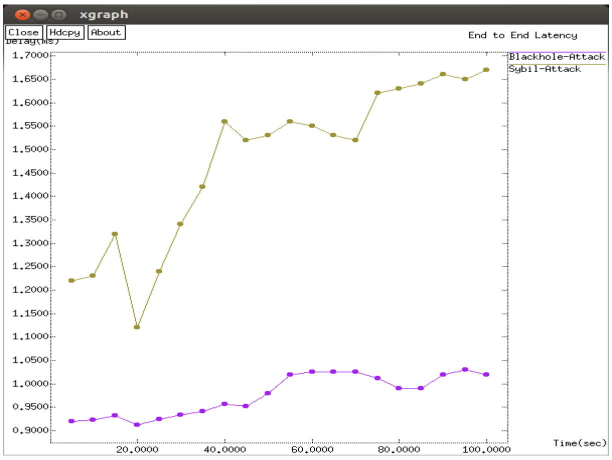


**Fig. 8:** Performance Analysis of End-to-End Latency.

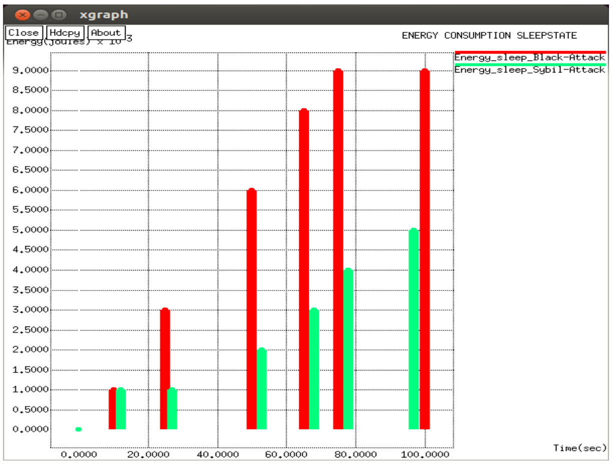


**Fig. 9:** Performance Analysis of Energy Consumption at Sleep State.

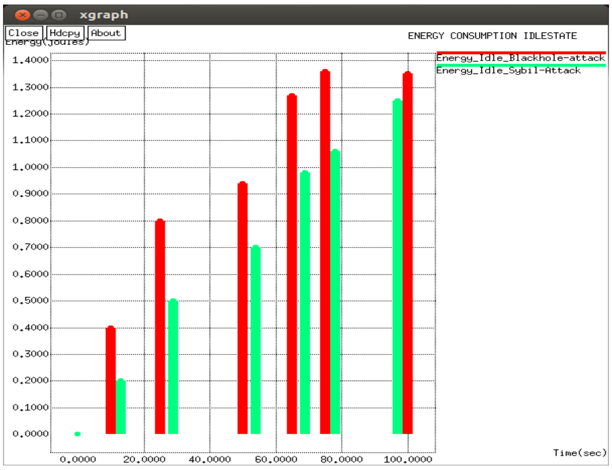


**Fig. 10:** Performance Analysis of Energy Consumption at Idle State.

Fig [6] shows the analysis of the packet delivery ratio, Fig [7] shows the consumption of network energy and Fig [8] shows the latency of the end to end in the network. The analysis of sleep and idle state of the network energy consumption is shown in Fig [9] and Fig [10], respectively.

## 5. Conclusion

In this paper, an anomaly based intrusion detection approach is proposed and implement in MANET. An enhanced replica detection scheme based on SPRT is proposed for mobile networks. In order to demonstrate the limitations of attacker strategies the proposed approach is applied to have secured path with average claims. The simulation results show that the technique quickly detects the mobile replicas with a small number of location claims. As well as, the performance of an average claim of the network is analyzed with the comparison of the true positive and negative values. So, that the performances prove that the efficiency of the proposed system have been improved than the existing.

## References

[1] Tao Shu and Marwan Krunz, “Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks”, IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 14, NO. 4, APRIL 2015

[2] Ayesha Taranum, Manju N, Tejaswini R M, “RAACK-Reinforce Adaptive Acknowledgement A Secure Intrusion Detection System for MANETs”, International Journal of Computer Science and Information Technology Research, Vol.2, Issue 2, 2014, pp.283-296.

[3] Michael Riecker, Sebastian Biedermann, Rachid El Bansarkhani and Matthias Hollick, “Lightweight energy consumption-based intrusion detection system for wireless sensor networks”, International Journal of Information Security, Springer, 2014, pp.1-8.

[4] Pu Cheng, Minghua Zhu, Xianzhong Liu, “Distributed T-Distribution-Based Intrusion Detection in Wireless Sensor Networks”, Springer, Vol.295, 2014, pp.313-323. https://doi.org/10.1007/978-3-642-54174-2_28.

[5] Francesco Buccafurri, Luigi Coppolino, Salvatore D’Antonio, Alessia Garofalo, Gianluca Lax, Antonino Noccera, Luigi Romano, “Trust-Based Intrusion Tolerant Routing in Wireless Sensor Networks”, Springer, Vol.8666, 2014, pp.214-229. https://doi.org/10.1007/978-3-319-10506-2_15.

[6] Wenchao Li, Ping Yi, Yue Wu, Li Pan, and Jianhua Li, “A New Intrusion Detection System Based on KNN Classification Algorithm in Wireless Sensor Network”, Journal of Electrical and Computer Engineering, Hindawi Publication, 2014, pp.1-9.

[7] K.Ankush, P.Ravindra and D.Krishna, “A Secure Intrusion-Detection System for Ad hoc mobile wireless networks”, International Journal of Embedded and Software Computing, Vol.5, 2014, pp.528-531.

[8] Poongothai and K.Duraiswamy, “Cross Layer Intrusion Detection System of Mobile Ad Hoc Networks using Feature Selection Approach”, WSEAS Transactions on Communications, Vol.13, 2014, pp.71-79.

[9] E.M.Shakshuki, Nan Kang, T.R.Sheltami, “EAACK – A Secure Intrusion Detection System for MANETs”, IEEE Transactions on Industrial Electronics, Vol.60, Issue 3, 2013, pp.1089-1098. https://doi.org/10.1109/TIE.2012.2196010.

[10] Gerrigagoitia, K. Uribeetxeberria, R., Zurutuza, U. and Arenaza, I., “ Reputation based Intrusion Detection System for Wireless Sensor Networks”, IEEE Communications on Complexity in Engineering, 2012, pp.1-5

[11] Peyman Kabiri and Mehran Aghaei, “Feature Analysis for Intrusion Detection in Mobile Ad-hoc Networks”, International Journal of Network Security, Vol.12, No.1, PP.42-49, Jan. 2011

[12] Chong Eik Loo, Mun Yong Ng, Christopher Leckie and Marimuthu Palaniswami, “er 2006: pp. 1–27 Intrusion Detection for Routing Attacks in Sensor Networks”, International Journal of Distributed Sensor Networks, Vol.2, 2006, pp.313-332. https://doi.org/10.1080/15501320600692044.

[13] John S. Baras, Svetlana Radosavac, George Theodorakopoulos, Dan Sterne, Peter Budulas and Richard Gopaul, “INTRUSION DETECTION SYSTEM RESILIENCY TO BYZANTINE ATTACKS: THE CASE STUDY OF WORMHOLES IN OLSR”, Research supported by the U.S. Army Research Laboratory under the Collaborative Technology Alliance Program, Cooperative Agreement DAAD19-01-2-0011.