Bulletin of Environment, Pharmacology and Life Sciences
Bull. Env. Pharmacol. Life Sci., Vol 4 [8] July 2015: 53-61
©2015 Academy for Environment and Life Sciences, India
Online ISSN 2277-1808
Journal's URL:http://www.bepls.com
CODEN: BEPLAD
Global Impact Factor 0.533
Universal Impact Factor 0.9804

ORIGINAL ARTICLE **OPEN ACCESS**

Presentation of Intrusion detection system for MANET networks Based on clustering

[1]Somayeh Khorramfar, [2]Reza Ahsan
Department of information Technology, Taali Institute of Higher Education, Qom, Iran
*E-mail: sara_khoramfar@yahoo.com
Department of computer engineering, College of Engineering, Qom Branch, Islamic Azad University, Qom, Iran

ABSTRACT

Now a days the mobile ad hoc network (MANET) has become one of the major research topics. It has features such as a lack of required infrastructure, speed up the establishment of the network, no need for centralized management, which increased the popularity of the network and its application in various fields. Security is one of the key aspects of the network. Intrusion Detection System is one of the strategies that have been used to secure the network. The clustering-based intrusion detection system because of its features such as scalability of the network is very popular. MANET's are highly vulnerable to attacks due to the open medium, dynamically changing network topology, cooperative algorithms, lack of centralized monitoring and management point, and lack of clear line defense. Therefore, in this paper intrusion detection system based on clustering with the ability to detect the presence of coalition provided which enables the coalition, detection rates and reduce false detection. The used idea is analysis trusts received from member nodes using Clustering data mining technique to determine the coalition nodes.

Keywords*: Mobile ad hoc networks (MANET), Clustering, MANET Attacks, and Security*

Received 01.05.2015 Revised 21.06.2015 Accepted 30.06. 2015

INTRODUCTION

A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. Ad hoc is Latin and means "for this purpose"[1]. MANET has received great attention in recent years, mainly due to the evolution of wireless networking and mobile computing hardware that made possible the introduction of various applications [2]. Often quoted MANET applications include battlefield and disaster relief. Each network node can directly communicate with nodes that are in the frequency range, so that need routing nodes in the network are operating in a distributed manner. In other words, if the source and destination nodes are not in the frequency range of each other, intermediate nodes should as navigation established the relationship between them. Figure 1 is an example of MANET.

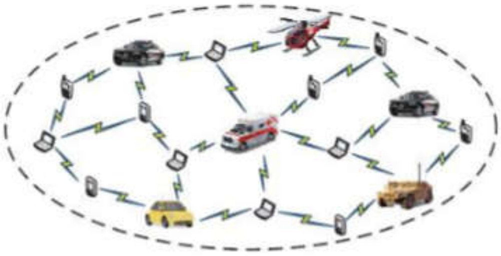

Figure 1: An example of MANET [3]

There are several characteristics that distinguish a MANET from other networks such as: - Open and shared transmission media - Connective dynamic -self and lack of infrastructure [4] - heterogeneity of nodes [4] -Limit the power consumption -Processing power, memory and bandwidth limits -Low Physical Security [4]. A numbers of applications this network as follows: 1. Conferencing 2 home and office networks 3.The rescue operation 4.Tablet 5.Military Operations 6. The sensor network 7. Vehicular Ad Hoc Network (VANET) [5].In the following some of the challenges facing the MANET presented: 1.Energy Management 2.Scalability Network 3.Routing 4.Control topologies 5.Security.

Attacks in MANET can be classified as Passive and Active Attacks. Passive attack is very difficult to detect because the operation of the network is not affected by this type attack. In active attack the intruders can modify the packets, inject the packets, drops the packet, or it can use the various feature of the network to launch the attack. Active attacks are very dangerous [6, 7]. Security Solutions of the MANET is divided in two types of encryption and intrusion detection system [8, 9].

Many clustering schemes have been proposed for MANET. The idea behind clustering is to group the network nodes into a number of overlapping clusters. Clustering makes possible a hierarchical routing in which paths are recorded between clusters instead of between nodes. A number of possible architectures of intrusion detection techniques in MANET have been proposed. These include stand-along intrusion detection, distributed and cooperative intrusion detection, and hierarchical intrusion detection [10, 11]. Since a cluster structure is a typical hierarchy, many papers focus on presenting an effective and efficient clustering scheme for MANET. The intrusion detection system architecture based on hierarchical clustering is used as intrusion detection system.

In clustering, the MANET is divided into several clusters and each cluster usually includes a clusterhead and a set of nodes. Inside the cluster, there are ordinary nodes also that have direct access only to this one clusterhead, and gateways. Gateways are nodes that can hear two or more clusterheads. Ordinary nodes send the packets to their clusterhead that either distributes the packets inside the cluster, or (if the destination is outside the cluster) forwards them to a gateway node to be delivered to the other clusters (Figure 2).

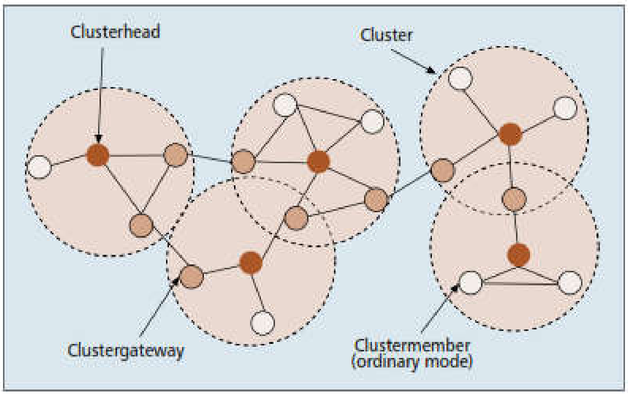

Figure 2: Cluster heads, gateways and ordinary nodes in MANET clustering

Since there is not centralized management of network infrastructure and tasks performed in a distributed manner, Reliance on the information to other nodes in the decision could be vulnerable in these networks. Therefore, it need to Trust mechanisms for accuracy of information received from other network nodes. Trust mechanisms for determining the amount of the trust to a node can use direct trust to a node, trust reports from other nodes or combination of these two methods. The Coalition attacks, one of the problems that threaten the Trust mechanisms in the report the trust of the other node in the MANET. Where multiple nodes together to create coalition and false reports are transmitted on an appropriate node and trust is a trust mechanism confused about the proper nodes.

According to the previous methods of intrusion detection network attacks has been off-set and less attention has been in inside of attacks, providing a new way to detect network attacks that are caused by the coalition nodes in the network is necessary. Therefore, in this paper intrusion detection systems based on clustering with the ability to detect the presence of coalition provided which enables the coalition, detection rates and reduce false detection. The used idea is analysis trusts received from member nodes using Clustering data mining technique to determine the coalition nodes.

MATERIALS AND METHODS

Intrusion detection system based on clustering, intrusion detection is the responsibility of cluster head node. Important subject in this way is needed to check reports received from member nodes.

In this article, intrusion detection systems based on clustering provided where in it with coalition diagnosis between member nodes and consider it in the process of self-assessment and global intrusion detection prevented from creation disorder inside the intrusion detection system by node Coalition.
Clustering is done on the basis of clustering algorithms and the parameters specified for it and the human factor is not involved in this matter.

Clustering process

Clustering involves four steps and shown in Figure 3. [10]

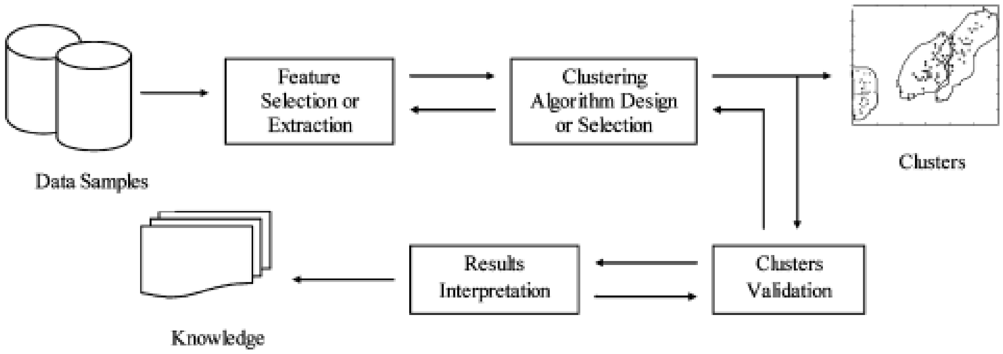
Data Samples
Feature Selection or Extraction
Clustering Algorithm Design or Selection
Clusters
Clusters Validation
Results Interpretation
Knowledge

Figure 3: Clustering processes

1. Selection and extraction of criteria, 2.Selection and design of clustering algorithms, 3. Clustering Validation, 4. Interpretation of results

Similarity measure

Commonly used for similar data Euclidean distance measure or other similar function, including the criteria can be outlined as follows:

$$\mathrm{d}(\mathbf{p},\mathbf{q}) = \sqrt{(p_1-q_1)^2+(p_2-q_2)^2+\cdots+(p_n-q_n)^2} = \sqrt{\sum_{i=1}^{n}(p_i-q_i)^2}$$

Where p, q are two points n-dimensional.
In information retrieval, cosine similarity is a commonly used similarity measure, defined on vectors arising from the bag of words model. In machine learning, common kernel functions such as the RBF kernel can be viewed as similarity functions

$$\text{similarity} = \cos(\theta) = \frac{A\cdot B}{\|A\|\|B\|} = \frac{\sum_{i=1}^{n} A_i \times B_i}{\sqrt{\sum_{i=1}^{n}(A_i)^2} \times \sqrt{\sum_{i=1}^{n}(B_i)^2}}$$

Clustering algorithms

It can be described as follows: [11]
1. First, the data consider as a separate cluster. The adjacency matrix calculates containing all the data.
The rows and columns of adjacency matrix include all data available.
If two clusters merged rows and columns of matrix corresponding to clusters are also integrated.
2. The based on method used to determine the similarity of the two clusters found close together and they will merge. 3. Adjacency matrix updates Dates for cluster integration. 4. Steps 2 and 3 will continue until the number of clusters to reach the desired number.

Characteristics of the proposed system

1 based on the cluster:
2. Recognition of the partnership:
3. Use a coalition detection mechanisms:
In the main idea of the proposed method add a coalition detection module to intrusion detection system to check reports received from Members and recognize the possibility of a coalition between them. General architecture of the proposed method is shown in Figure 4.

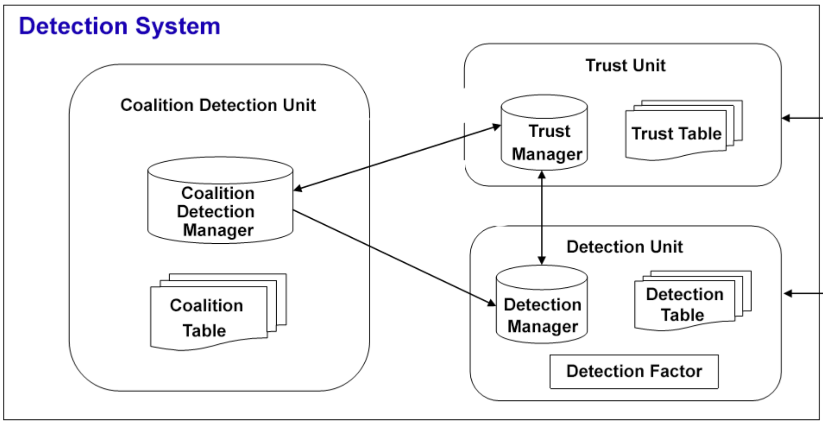

Figure 4: Intrusion detection architecture of the proposed system

The nodes of member in the proposed method are Contains two units Recognize and trust. Criteria considered for detect abuses in nodes of member is as follows:

The number of interactions with the target node is more of the number of predetermined threshold INTRACTION_NEEDED_THRESHOLD. This measure is intended to the other criteria are taken from other nodes.

A confidence level for the target node is lower of the threshold INTRUSION_TRUST_THRESHOLD.

In the proposed method, each node has a table of trust that confidence node it to the other members is maintained. Unit trust based on positive and negative interactions with other nodes is Level of trust in the trust holds a node in the trust table. The trust calculated from the following equation to calculate the trust is used, is achieved. Values confidence calculated are at range {-1, 1}:

If DTi,j(t)>0 and PI then

$$DTi,j(t+1)= DTi,j(t)+ \alpha D(i)(1- DTi,j(t))$$

If DTi,j(t)<0 and PI then

$$DTi,j(t+1)= DTi,j(t)+ \alpha D (i))/(1-min(|DTi,j(t)|-| \alpha D (i)|)$$

If DTi,j(t)>0 and NI then

$$DTi,j(t+1)= DTi,j(t)+ \beta D(i)(1- min(|DTi,j(t)|-| \beta D (i)|)$$

If DTi,j(t)<0 and NI then

$$DTi,j(t+1)= DTi,j(t)+ \beta D (i))(1+DTi,j(t))$$

where NI, PI represent the positive and negative interactions with node i and j. Also $\alpha D (i)> 0$ and $\beta D (i) <0$ is effective coefficients in changing confidence calculated.

Table of confidence for member nodes are as follows, where in it, Target: the address of the target node, Trust Value: The calculated amount of trust for that node, and Neg.Interaction and Pos.Interaction are the number of positive and negative interactions with that node, respectively.

Target ID	Trust Value	Neg.Interaction	Pos.Interaction

Cluster head node

This node has three units of detection, trust and detection of coalition.

Detection of cluster head node is as a member node that has its own local detection unit and by monitoring the adjacent nodes perform local detection. For intrusion detection according calculated confidence, it used to be three levels of trust defined for each node which can be seen in Table 1:

Table 1: Classification of member nodes based on confidence

Condition	The level of confidence
Trust≥SAFE_THRESHOLD	Reliable
INTRUSION_ THRESHOLD< Trust< SAFE_THRESHOLD	Unknown
Trust≤INTRUSION_ THRESHOLD	No confidence

Confidence unit for each node calculates the two types of confidence: DT direct Confidence and Confidence control WT. Values confidence calculated are at range {-1,1}:

Reporter ID	Target ID	Trust Value

Where in Reporter ID: reporting node ID, Target ID: ID of the target node, Trust Value is the Confidence stated.

To calculate the trust control trust unit using received trusts from member nodes based on reports received from the detection of the coalition calculated some of users generally trust to the desired node. This amount is called social credibility of witnesses and it obtained by following equation:
Mem (φ (DTi, j) opinion (j, k) = WR I, k (t)

$$WR_{I,k}(t) = \frac{\sum_j \in Mem\ (\varphi\ (DT_{i,j})\ \times opinion(j,k)}{\sum_j \in Mem\ \varphi}$$

Which Mem is set members that have expressed their trust and based on reports of detection of the coalition is not a coalition and also opinion (j, k) is expressed trust by node j about node k, Also φ is calculated as follows:

$$\varphi(r) = \begin{cases} 0 & -1 \leq r < INTRUSION\_THRESHOLD \\ \dfrac{r - INTRUSION\_THRESHOLD}{SAFE\_THRESHOLD - INTRUSION\_THRESHOLD} & INTRUSION\_THRESHOLD \leq R < SAFE\_THRESHOLD \\ 1 & SAFE\_THRESHOLD \leq r < 1 \end{cases}$$

where INTRUSION_THRESHOLD and SAFE_THRESHOLD are threshold values.
Coalition detection unit is responsible review reports received from member nodes about the level of trust to other nodes and detection coalition between them. In the proposed system, each node monitors on the behavior of neighboring nodes and in case of mistreatment notice to cluster head by sending a message to the cluster: Attack_Alarm_msg. The message is as follows:
→ Attack_Alarm_msg (Member Cluster head)
{Reporter ID, target ID}
The above structure indicates the message sent from node member to cluster head node. When a cluster head node receives message "Attack_Alarm_msg", intrusion detection process begins at global cluster. Cluster head will be waiting amount threshold "Wait_For_ Response" and the message "Trust_ declaration_Req" is as follows:
Trust_ declaration_Req (Cluster head → Members)
{target ID}
The message is contains the address suspected node.
In response to this request, each node must be in the form of a message "Trust_declaration_Resp" send your trust level than node suspected for cluster head. "Trust_ declaration_Resp" structure is as follows:
Trust_ declaration_Resp(Members Clusterhead)
{Reporter ID, target ID}

After review of the trust units on the basis of reports received recognition coalition and according to which the coalition detection unit receives about possible coalition calculate the amount of trust cluster. The detection unit according to trusts calculated from unit trust decides about influential report received
If approved report, message "Intrusion_Detected_ msg" sent to all cluster nodes except nodes
have been identifiedat detection process coalition as a member of the coalition node. The structure of this message is as follows:
Intrusion_Detected_ msg (Cluster head non_colluding Members)
target ID
where The target ID is ID of attacked node.

RESULTS AND DISCUSSION

The results of the simulation using the C # programming language are studied. Network includes 40 nodes and a cluster head as the cluster management. Ambient temperature is the duty of every node. The ambient temperature was 25 degrees in default. Figure 5 shows a view of the network nodes.

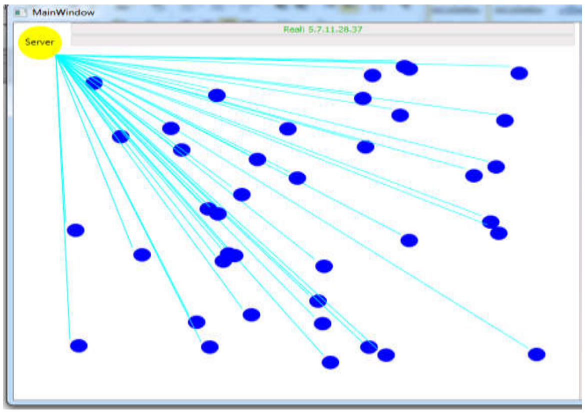

Figure 5: The view of the network nodes.

Simulation was carried out for the different cases by changing the following factors: 1.The position of nodes, 2.The number of nodes in coalition, 3.change of threshold, 4.change of α and β. The results were as follows.

1. The position of nodes

a) The regular nodes:

Simulation was repeated 10 times in two cases normal and optimal detection of intruders. On average, in normal case, simulation time 23 seconds, intrusion detection 42% and overhead rate is 8.7%. In case of optimal detection of intruders simulation time 15 seconds, intrusion detection 100% and overhead rate is 9.7%. In the following comparison between normal and optimal detection of intruders was shown in Figures 6-8 in the regular nodes.

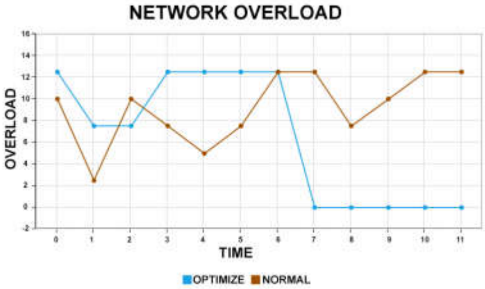

Figure 6: Comparison of overload between normal and optimal detection of intruders

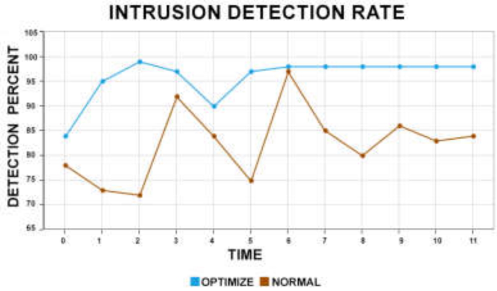

Figure 7: Comparison of intrusion detection between normal and optimal detection of intruders

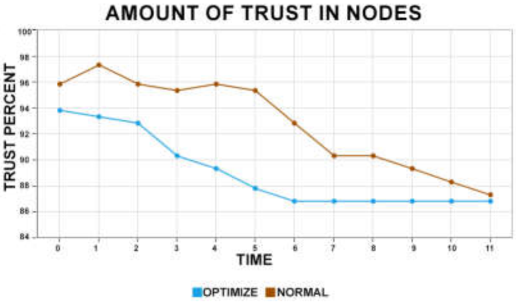

Figure 8: Comparison of the trust in the nodes between normal and optimal detection of intruders

b) The mobile nodes:

Simulation was repeated 10 times in two cases normal and optimal detection of intruders. On average, in normal case, simulation time 25 seconds, intrusion detection 100% and overhead rate is 8.5%. In case of optimal detection of intruders simulation time 23 seconds, intrusion detection 100% and overhead rate is 9.5%.

c) The fixed position by mobility nodes:

Simulation was repeated 10 times in two cases normal and optimal detection of intruders. On average, in normal case, simulation time 25 seconds, intrusion detection 100% and overhead rate is 8.5%. In case of optimal detection of intruders simulation time 13 seconds, intrusion detection 100% and overhead rate is 9.7%.

2. The number of nodes in coalition

The simulation of the number of nodes coalition was carried out in two cases and the results presented by figures.

a) Confederate nodes are 10%:

Simulation was repeated with 10 Confederate nodes in two cases normal and optimal detection of intruders in Time = 40s.The average of the results simulation is as follows.

In normal case, simulation time 36.9 seconds, intrusion detection 77.2% and overhead rate is 16.45%. In case of optimal detection of intruders simulation time 22.6 seconds, intrusion detection 97% and overhead rate is 17.68%.

In the following comparison between normal and optimal detection of intruders was shown in Figures 9-11.

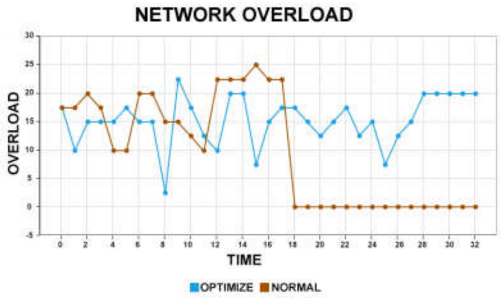

Figure 9: Comparison of overload between normal and optimal detection of intruders

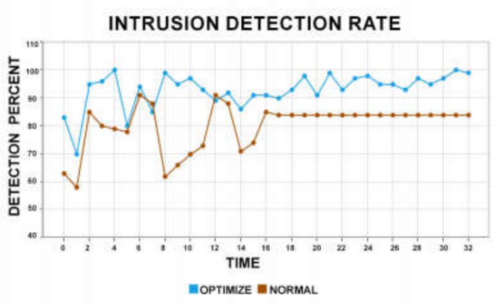

Figure 10: Comparison of intrusion detection between normal and optimal detection of intruders

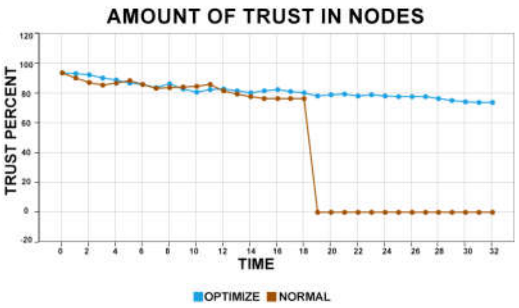

Figure 11: Comparison of the trust in the nodes between normal and optimal detection of intruders

b) Confederate nodes are 50%:

Simulation was repeated with 20 confederate nodes in two cases normal and optimal detection of intruders in Time = 40s.The average of the results simulation is as follows.

In normal case, simulation time 40 seconds, intrusion detection 76.4% and overhead rate is 32.66%. In case of optimal detection of intruders simulation time 26.2 seconds, intrusion detection 98.5% and overhead rate is 33.46%.

c) Confederate nodes are more than 50%:

Simulation was repeated with 30 confederate nodes in two cases normal and optimal detection of intruders in Time = 40s.The average of the results simulation is as follows.

In normal case, simulation time 40 seconds, intrusion detection 74.1% and overhead rate is 49.4%. In case of optimal detection of intruders simulation time 23.9 seconds, intrusion detection 98.7% and overhead rate is 49.13%.

3. Change of threshold

Simulation was repeated with INTERUSION_THRESHOLD=0.1 and SAFE_THRESHOLD=0.9 in two cases normal and optimal detection of intruders in Time = 30s.The average of the results simulation is as follows.

In normal case, simulation time 23.5 seconds, intrusion detection 68% and overhead rate is 8.51%. In case of optimal detection of intruders simulation time 19.1 seconds, intrusion detection 98% and overhead rate is 8.48%.

In the following comparison between normal and optimal detection of intruders was shown in Figures 12-14.

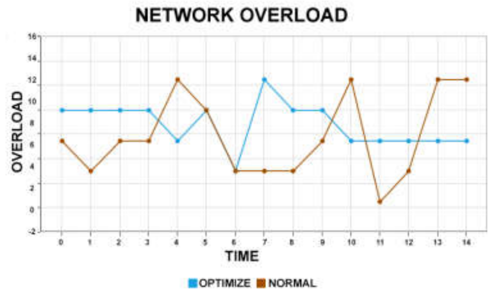

Figure 12: Comparison of overload between normal and optimal detection of intruders

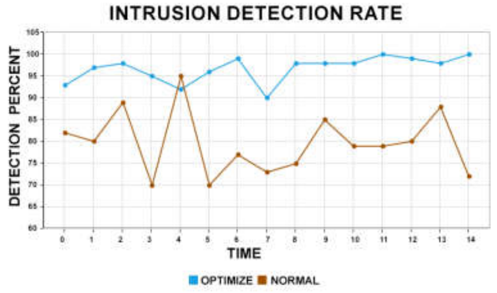

Figure 13: Comparison of intrusion detection between normal and optimal detection of intruders

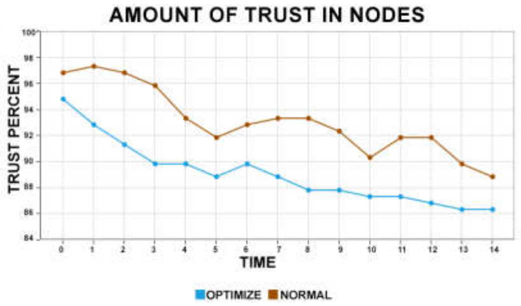

Figure 14: Comparison of the trust in the nodes between normal and optimal detection of intruders

4. Change of α and β

Simulation was repeated with changing the amounts of α = 0.1 and β = -0.1 in two cases normal and optimal detection of intruders in Time = 20s.The average of the results simulation is as follows.

In normal case, simulation time 19.8 seconds, intrusion detection 60% and overhead rate is 7.41%. In case of optimal detection of intruders simulation time 18.2 seconds, intrusion detection 88% and overhead rate is 8.79%.

In the following comparison between normal and optimal detection of intruders was shown in Figures 15-17.

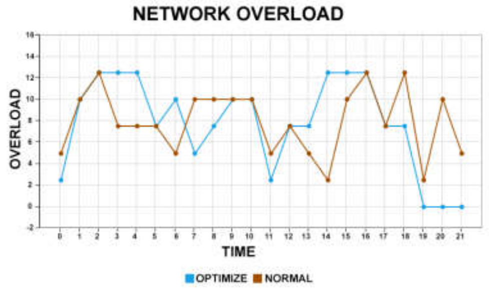

Figure 15: Comparison of overload between normal and optimal detection of intruders

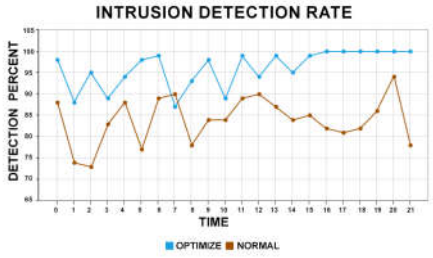

Figure 16: Comparison of intrusion detection between normal and optimal detection of intruders

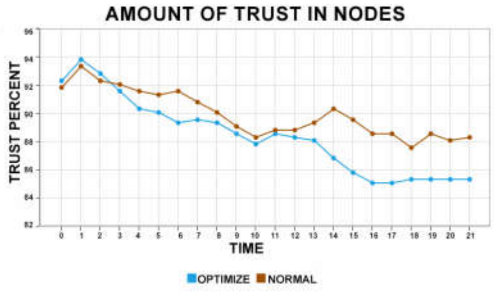

Figure 17: Comparison of the trust in the nodes between normal and optimal detection of intruders

CONCLUSION

In this paper intrusion detection systems based on clustering with the ability to detect the presence of coalition provided which enables the coalition, detection rates and reduce false detection. The used idea is analysis trusts received from member nodes using Clustering data mining technique to determine the coalition nodes. By using of trust table increased recognizing the devastating coalition nodes.It is clear that using this mechanism, there is more control over the performance of nodes and rigor is more on the behavior of nodes. By adopting this mechanism, the identification of malicious nodes within the MANET increased close to 99% and network overhead up to 5%.

REFERENCES

1. Sheikh, R, Singh Chande, M. and Kumar Mishra, D., (2010). "Security issues in MANET: A review" in 7th International Conference On Wireless And Optical Communications Networks (WOCN'10),pp.1-4.
2. Chlamtac, I2 Conti, M. and Liu, J. J. N.,(2003). Mobile ad hoc networking: imperatives and challenges" Ad Hoc Networks, vol. 1, pp. 13-64.
3. Kandah, F., Singh, Y, and Chonggang, W., (2011)."Colluding injected attack in mobile ad-hoc networks" in IEEE Conference on Computer Communication Workshops (INFOCOM WKSHPS' 11), pp.235-240.
4. Giordano, S. and Lu, W. W., "Challenges in mobile ad hoc networking" IEEE Communications Magazine, vol . 39, pp.129-130, 2001.
5. Perkins, C, E., Ad Hoc Networking: Addison-Wesley Professional, 2008.
6. Wu, B., Chen, J., Wu, J. and Cardei, M., " A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks" Wireless Network Security, Signals and Communication Technology, Springer US, pp. 103-135, 2007.
7. Salehi-abari, A. and white, t., "Witness-Based Collusion and Trust-A ware Societies" in International Conference on Computational Science and Engineering (CSE' 09), vol.4, pp. 1008-1014, 2009.
8. Wu, B., Chen, J., Wu, J. and Cardei, M., " A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks" Wireless Network Security, Signals and Communication Technology, Springer US, pp. 103-135, 2007.
9. Anantvalee, T. and Wu, J., " A Survey on Intrusion Detection in Mobile Ad Hoc Networks" Wireless Network Security, Signals and Communication Technology Y. Xiao, X. S. Shen and D.,Z. Du, eds.,Springer Us, pp. 159-180,2007.
10. Rui, X. and Wunsch, D., II, "Survey of clustering algorithms" IEEE Transacation on Neural Networks, vol. 16,pp. 645-678, 2005.
11. Rui, X. and Wunsch, D., II, "Survey of clustering algorithms" IEEE Transacation on Neural Networks, vol. 16,pp. 645-678, 2005.

CITATION OF THIS ARTICLE

Somayeh K, Reza A. Presentation of Intrusion detection system for MANET networks Based on clustering. Bull. Env. Pharmacol. Life Sci., Vol 4 [8] July 2015: 53-61