Trust Aware Intrusion Detection System based on Cluster

Devendra Singh
Department of Computer Science & Engineering
IFTM University, Moradabad, India.

S.S. Bedi
Department of CS&IT
MJPR University, Bareilly, India

ABSTRACT
Mobile Ad hoc Networks (MANET) has gained substantial research interest, owing to its easy deployment and inexpensiveness. However, the security of the network is the major concern, because of the absence of the central authority. This work addresses these issues by incorporating the trust mechanism in the cluster formation and routing. The chief node is selected on the basis of four trust parameters such as energy, packet delivery ratio, neighbour count and mobility. The chief node kicks off the misbehaving nodes during the process of routing. The proposed work is proved to be resilient against replay and sybil attacks. The performance of this work is evaluated in terms of several popular performance metrics and the system proves its efficacy.

Keywords
MANET, trust, routing, replay attack, sybil attack.

1. INTRODUCTION
Mobile Ad hoc Network (MANET) is a group of mobile nodes, which can perform bi-directional communication in a wireless fashion. Every mobile node acts both as a transmitter and receiver. The communication can take place either directly or indirectly. The direct communication can happen directly between the source and the destination. Indirect communication is made possible with the help of the intermediary nodes, through which the source and the destination node can communicate.

MANET doesn't follow a static infrastructure and thus the concept of base station or access points is absent. This characteristic feature of quick deployment makes it suitable to many emergency applications such as military and healthcare applications. On the other hand, the same characteristic feature makes it vulnerable to several kinds of attacks by the adversaries.

This kind of networks follow distributed architecture which makes it easier for the intruders to inject new malicious nodes and to perform unwanted activities. The threatening intruding activities has to be prevented or atleast detected by some mechanism. Intrusion detection is the second line of defence mechanism to combat against intrusion.

However, introduction of Intrusion Detection System (IDS) in MANET is a challenging, as there is no access point. Thus, a node can execute its own IDS to ensure security [1-4]. This is not feasible because of the increased energy consumption, which in turn reduces the lifetime of the network. Besides this, the mobile nodes are energy restricted.

Besides this, it is not a good idea to retain the same node as the chief node for a long time, as it may deteriorate the energy of a single node. Thus, cluster recycling process is necessary, such that the eligible node will then be selected as a chief node. Chief node selection itself is a separate research area in MANET. The chief node can be selected in a random fashion or by connectivity [5, 6].

On realizing the importance of energy utilization, this work proposes a cluster based IDS for MANET. The main goals of the proposed work are to ensure security by detecting misbehaving nodes and to minimize the energy consumption and thereby maximizing the lifetime of the network. The concept behind clustering is that the chief node takes care of all the activities of its constituent nodes, which saves maximum energy.

This paper proposes a method which selects the chief node by means of trust measure. The trust measure is computed by taking energy, packet delivery ratio, number of neighbours and mobility into account. All the aforementioned four parameters decide the potentiality of a node. Thus, the proposed work selects the chief node by the computed trust measure and is recycled for every period of time. The overall flow of the work is presented in figure 1.

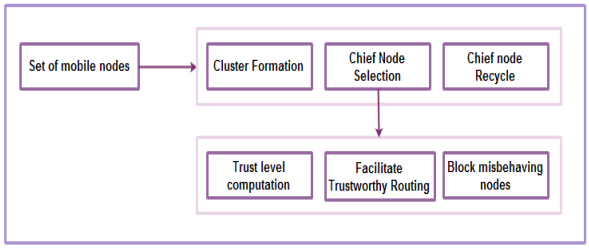

Figure1. Overall workflow of the proposed work

The chief node controls and monitors the behaviour of its constituent nodes. In case of any misbehaviour the chief node blocks that particular node, in order to ensure security. The chief node computes the trust value of all its constituent nodes and performs routing accordingly.

The experimental results of the proposed work prove its efficiency in terms of energy and routing, which paves way for eliminating the misbehaving nodes from the scenario. The packet delivery ratio and throughput of the system is considerably improved along with minimal end-to-end delay.

The work of this paper is organised as follows. In section 2 related literatures with respect to clustering and intrusion detection in routing is presented. The proposed work is described in section 3. The performance of the proposed work is evaluated in section 4. Finally, the concluding remarks are presented in section 5.

2. RELATED WORK
This section studies the existing literature with respect to clustering and intrusion detection in MANET.

2.1 Clustering in MANET

Clustering is the collection of nodes, consisting of cluster member node and cluster head node. Here cluster head node is the chief node. Chief node will be the monitoring node among each cluster. MANET faces many problems, as it has got no central authority. Clustering technique imitate the functionality of the fixed infrastructure, such that the nodes are controlled and monitored by some central authority. Every cluster has a head node and it is responsible for all activities of the cluster. However, choosing the right node as a cluster is a challenging task [7]. Some of the cluster head selection algorithms for MANET are lowest ID, highest degree, distributed clustering algorithm, weighted clustering algorithm, distributed weighted clustering algorithm [8 – 12]. Linked Cluster Algorithm is an algorithm that prompts each node to behave as a cluster head, gateway or simple nodes [8]. Initially, all the nodes are normal and each node broadcasts its own ID for every time period. In [13], an adaptive clustering algorithm in which all the nodes act in the same way, once the cluster is formed and the cluster head has no role to play. The algorithm proposed in [9] takes the connectivity of the nodes alone into account and the cluster head is selected. In [14], an algorithm namely associativity based cluster formation and management is proposed. This algorithm focuses on the stability of the node alone to elect the cluster head.

2.2 Detecting misbehaving nodes

Some of the intrusion detection techniques by the incorporation of clustering mechanism are observed in several works [15-19]. Intrusive behaviour can easily be pointed out with clustering, because the cluster head plays the role of local coordinator. In [20], a trust model for ad hoc networks is proposed based on clustering technique. In this model, the nodes are grouped into clusters and each cluster is managed by a cluster head. The trust relationship is computed between the nodes. In [21], the node's trust is calculated by focusing the packet delivery ratio and the path is computed. The work proposed in [22] focuses on routing misbehaviours. The main attributes considered by this work are trust, motion pattern, hop count and activity level. The simulation is carried out with DSR protocol.

3. CLUSTER BASED IDS

The proposed methodology of cluster based IDS for MANET is compartmentalized into chief node selection, chief node recycling process and trustworthy routing. The first step is to select the most appropriate node as chief node. The selected chief node is recycled for every period of time, in order to conserve the energy of that node. The elected cluster head computes the trust level of all its' constituent nodes and tends to carry out the process of routing accordingly. All these phases are explained in the forthcoming sections.

3.1 Chief node selection

This process is given more importance, as the chief node must be trustworthy and has to be capable of managing all its' constituent nodes. The chief node is picked out by means of trust parameters such as energy, packet delivery ratio, neighbour count and mobility and is illustrated in figure2. To select the chief node energy is important parameter for its long survival in network, packet delivery ration signify the performance of that node in the network, neighbor count means connectivity of node in the network and last mobility parameter is to minimize the change in topology. Because of different parameters used in calculating trust, normalization between these parameters must be needed. Because of this reason all parameters calculated between 0 to 1.

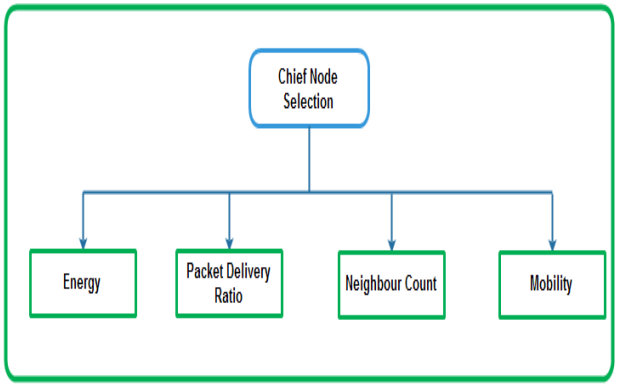

Figure2. Trust parameters for chief node selection

3.1.1 Energy[ε]

Energy plays a crucial role in computing the trust level of nodes. This is because an energy drained node cannot serve the purpose. Thus, energy is considered as the primary parameter. A fully keyed up node is given the value 1 and void energized node is assigned with the value 0. The value of this parameter varies from 0 and 1, based on the energy of any node in table1.

Table 1. Energy table

Energy value	Node type
0	Zero energized
0.5	Moderately energized
0.75	Three-fourth energized
1	Energy packed node

*3.1.2 Packet delivery ratio[**P**]*

The packet delivery ratio determines the behaviour of the node, which makes sense that the incoming and the outgoing packets are taken into account. For instance, a node may not forward all the packets it receives, to the destination or a node may duplicate packets and forward the same. Both these cases illustrate the attitude of misbehaving nodes, which needs to be eliminated. This case can be explained by the following scenario.

Let x be the count of incoming packets and y be the count of outgoing packets. The node is claimed as normal behaving node when the following condition satisfies.

$$x = y \quad (1)$$

This makes sense that the count of incoming packets is equal to the outgoing packets and this case is very normal. The scenario of the misbehaviour of a node is illustrated by the following cases on eqn. 2, 3 and 4.

$$X = y/2 \quad (2)$$

$$X = 2y \quad (3)$$

$$X = 0y \quad (4)$$

Eqns 2, 3 and 4 demonstrate the misbehaviour of a node. Eqn. 2 illustrates the case that the node forwards only half of the packets it received. This might be due to the nodes selfishness. In the second case eqn3, the nodes forward twice the count of the received packets. This makes sense that the node intends to replay the same packet over and over again.

This is considered as a serious issue because of energy restriction in mobile nodes. This type of packet forwarding results in the energy depletion and in turn death of a node. The final case eqn4 exemplifies the scenario, in which the node pays no attention towards packet transformation. The reasons for this zero forwarding can be the node failure or link failure. This work rates the nodes with respect to packet delivery ratio by giving 1 to the normal nodes and 0 to all the misbehaving nodes, as illustrated in eqn. 2, 3 and 4.

3.1.3 Neighbour count [η]

The neighbour count is another important parameter to compute trust level. A node with many neighbour nodes is observed to serve its purpose perfectly. Thus, a node is rated as healthy with respect to the count of neighbour nodes. The nodes are categorized as weak, fit, strong and strongest on the basis of the count of neighbours given in table2. The count of neighbours of all the nodes is calculated and arranged in descending order. The node with maximum number of neighbours is rated as 1 and the node with least number of neighbours is rated as 0.

Table 2. Neighbour_count table

Ranked Neighbour value	Node type
0	Weak
0.5	Fit
0.75	Strong
1	Strongest

3.1.4 Mobility [μ]

Final parameter being employed to compute trust value is mobility. The mobility model of a node is tracked, as a more dynamic node may result in service degradation. For this reason, this work considers mobility also. When the node is extremely mobile, then the mobility value of that node is assigned as 0. On the other hand, the value 1 is assigned to a steady node given in table3.

Table 3: Mobility table

Mobility value	Node type
0	Extremely mobile
0.5	Moderately mobile
0.75	Three-fourth mobile
1	Steady

3.1.5 Trust value computation

The trust value T of a node is computed by taking the mean of all the aforementioned parameters. The trust value is computed by the following equation.

$$T = \frac{\mathcal{E}+P+\eta+\mu}{4} \quad (5)$$

Where $\mathcal{E}$ is the energy, P is the packet delivery ratio, η is the neighbour count, μ is the mobility rate. By computing the T value, the node's level of trustworthiness can be rated and is given in table4 according to eqn5.

Table4. Node's behaviour

S.No	*T*	Nature of node
1	0.8 to 1.0	Trustworthy node
2	0.5 to 0.7	Partially trustworthy node
3	0-0.4	Malicious node

The T value of the nodes decides the chief node and the cluster are formed.

3.2 Chief node recycling process

It is not possible to maintain the same node as chief node for a longer period of time. The energy of the chief node will get depleted very fast, so it is necessary to preserve the energy of the chief node. This is possible only when the chief node is recycled then and there. Thus, the chief node is re-elected for every sixty seconds.

Chief node selection algorithm

Input : Set of nodes;
Output: Clusters
Begin
nod_thr=20;
For every 60 seconds
Randomly select a node;
Draw a circle which encloses 20 nodes;
if(node<20)
broadcast join request;
For each node in a cluster
Compute trust value by (5);
Arrange the trust values in descending order;
Select the first ranked node;
Declare the node as chief;
End;
End;

3.3 Trustworthy Routing

This work assumes that every node knows its neighbour and the nearby cluster. These details are stored in the neighbour_node and the neighbour_cluster tables respectively. Besides this, each chief node maintains the trust table of all its constituent nodes and this table maintains the trust level of all its constituent nodes.

Consider a scenario that a node needs to forward the packet to another node. The packet transmission is accomplished by the following procedure. Initially, the source node broadcasts the R_Req packet to the chief node. The chief node then checks whether or not the destination node is a constituent node of that particular cluster. In case, if the destination node is present in the same cluster, then the request is directed to it. Alternately, if the destination node is not a part of the cluster, then the chief node redirects the request to the neighbourhood clusters. Every node appends its own identifier to the packet, when the packet navigates through it. When the packet reaches the destination it replies the source node with the R_Rep. The routing cost is minimal in this case, as the routing overhead is handled by the cluster heads. Besides this the proposed work considers a larger cluster, so as to conserve more energy. As the cluster size is larger, several routes may exist between the source and the destination. The chief node selects the best route by taking the trust level into account. The chief node accomplishes this task by computing the occurrence frequency of trustworthy nodes in every possible route. This is computed by

$$t_{route} = \frac{count\ \ of\ \ trustwort\ \ hy\ nodes}{total\ \ number\ \ of\ nodes} \quad (6)$$

By this way, all the possible routes are evaluated. The routes are then rated from the worst to the best. This can be explained by the following. Let a be the total number of nodes and b be the count of trustworthy nodes.

$$a = b \quad (7)$$

$$b = \frac{a}{2} \quad (8)$$

$$b = 0 \quad (9)$$

In case, if the total number of nodes equals the count of trustworthy nodes, then the route is rated as the best. The second case have half the number of total nodes as trustworthy nodes and this route can be rated as fair route. In the worst case, if the route contains no trustworthy nodes along the path, then that route is considered as the worst.

By this way, the chief node excludes the worst route from the scenario and picks the best or fair route. This makes sense that all the non-trustworthy nodes are kicked off from the scenario. As far as this work is concerned, the malicious nodes may stimulate replay attacks and sybil attacks.

Routing algorithm

Begin

Source node forward R_Req to the chief node for the destination node;

Chief node checks the presence of destination node in its cluster;

If destination node present in cluster

Redirect the R_Req to the destination node;

Else

Redirect the R_Req to the neighbourhood chief node;

Append the node_id along the path in the packet;

Destination node replies R_Rep to the source node;

Compute all the possible routes;

Select the best route by (6)

End;

3.4 Solution to attacks

3.4.1 Replay attacks

Replay attacks are the most common attacks in which the malicious node tends to replay the packets being forwarded to it. The main objective of this attack is to deteriorate the performance of network by introducing network traffic and energy depletion. This leads to the death of nodes. The proposed work overcomes this attack by considering the packet delivery ratio. The chief node blocks the nodes with abnormal packet delivery ratio.

3.4.2 Sybil attacks

Sybil attacks are attacks in which the control packets are forwarded by using different identities. MANET is more susceptible to sybil attacks, as there is no central authority to manage the nodes. This work withstands such attacks by the employment of chief node, which manages the constituent nodes of the cluster.

The proposed work is resistive to replay and sybil attacks. Apart from this, the chief node is vigilant all the time, in order to hold down the activities of misbehaving nodes. Once the chief node computes the packet delivery ratio, the forwarding pattern of nodes is figured out. Based on the computed pattern, the misbehaving nodes can easily be figured out and the chief node blocks those misbehaving nodes.

The proposed work ensures security of the network by withstanding against replay and sybil attacks, performs trustworthy routing which improves the quality of system, conserves maximum energy and in turn improves the lifetime of the network as well.

4. EXPERIMENTAL ANALYSIS

The size of the network varies with respect to the number of nodes. The number of nodes is varied between 10 and 100. The size of the network ranges from $100 \times 100\ m^2$ to $1000 \times 1000\ m^2$. The nodes are placed in a randomly distributed manner. The random waypoint mobility model is exploited in this work and it makes sense that a mobile node remains in a location for a certain period of time, which is termed as 'pause'. After the time gets expired, the mobile node starts to choose a destination and the speed. Then, the node traverse towards the destination node at the chosen speed and again it will get paused. The maximum speed of the node of this work is 14m/sec. The node pause time is set as 20 seconds. AODV is employed as the routing protocol. The simulation parameters are presented in table 4 respectively.

Table 4: Simulation Parameters

Simulation parameters	Value
Node count	10 – 120
Network size	$100 \times 100\ m^2$ to $1000 \times 1000\ m^2$
Node placement	Random distribution
Routing protocol	AODV
Simulation time	1000 sec
Mobility pattern	Random waypoint
Node's motion speed	0 to 14 m/sec

NS2 is utilized for carrying out this simulation. The performance of the proposed work is evaluated in terms of packet drop ratio, detection accuracy, packet delivery ratio, energy consumption, network lifetime and throughput.

4.1 Packet drop ratio analysis

Packet drop ratio is the rate of packets that are dropped while packet transmission. The packet drop ratio must be preferably minimal, such that all the packets are transmitted promptly. Figure 3 depicts the experimental results of packet drop ratio with respect to mobility. Packet Drop Ratio is increasing with higher mobility due to fast changes in topology of network.

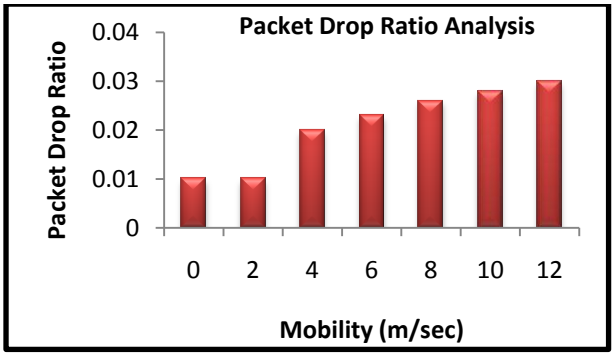

Figure3. Packet drop ratio analysis

4.2 Detection Accuracy

The chief node must catch the misbehaving nodes at the earliest, so as to prove the efficiency of the system. A system is claimed as efficient when the detection accuracy is maximal. The detection accuracy of the system is analysed with respect to mobility and varied count of malicious nodes in figure 4 and 5. Detection accuracy will decrease with increase in malicious node because more malicious node drops more packets in the network. Detection accuracy is reduced with increase in malicious nodes because connections in network associated with malicious nodes also increases and values for calculating trust in proposed method effects resulting accuracy. Detection will almost steady after certain mobility speed as in figure 5.

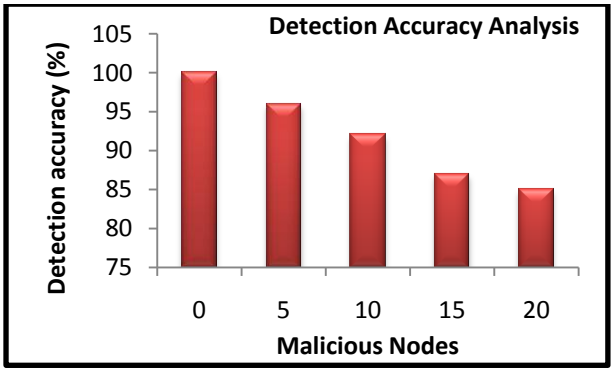

Figure4. Detection accuracy w.r.t malicious nodes

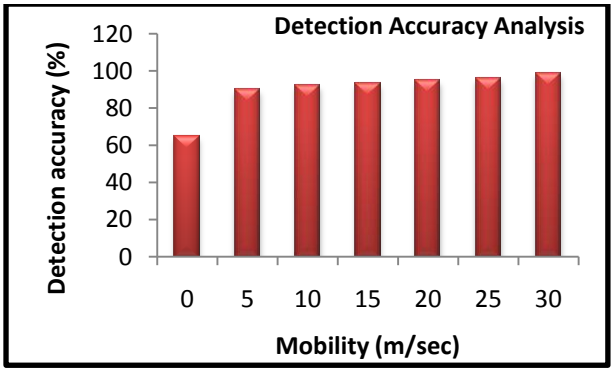

Figure5. Detection accuracy w.r.t mobility

4.3 Packet Delivery Ratio

Packet delivery ratio is the most important performance metric of a network. This metric decides the effectiveness of the system. Higher packet delivery ratio means the better performance of the system. This work analyses the packet delivery ratio with respect to mobility and varied number of malicious nodes. The experimental results are presented in fig 6 and 7 respectively. Packet delivery ratio is not decreasing fast as increasing in malicious node because PDR is one of parameter in calculating trust. Mobility also almost does not effect on PDR because chief node selected with low mobility value. Packet delivery ratio is almost invariant to the number of malicious nodes because chosen route in the network with the help of trusted nodes. Figure 7 clearly shows the packet delivery ratio 20 malicious node is almost 75%.

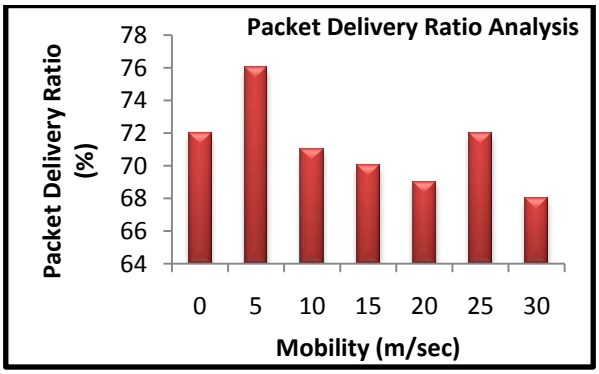

Figure6. Packet Delivery Ratio analysis w.r.t mobility

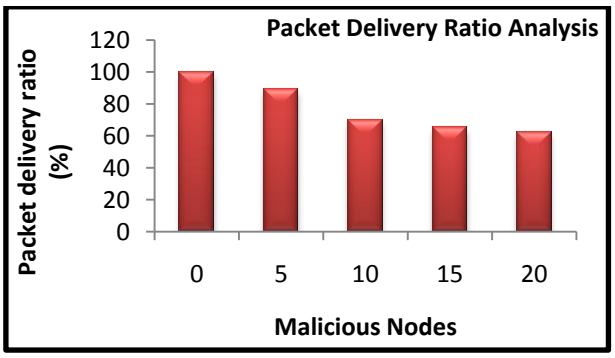

Figure7. Packet Delivery Ratio analysis w.r.t malicious nodes

4.4 Throughput

Throughput is the measure of successful packet delivery within the network. A system with maximum throughput is preferable for efficient communication. The throughput of the proposed work is presented in figure8. Throughput of this system is varied with mobility but still good with increasing mobility because all communication is passing through chief node and it is selected with lowest mobility in the network. However, if we increase malicious node in the network throughput will get decrease. Throughput is the important parameter because it demonstrates the input of attacks.

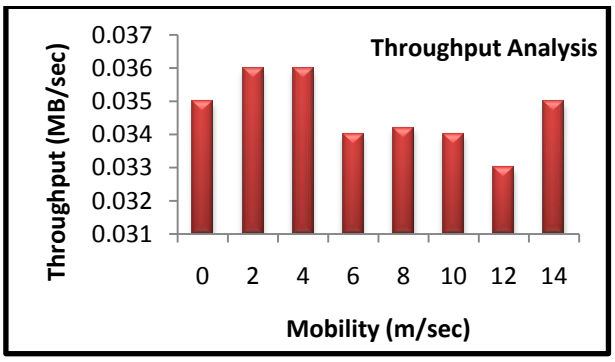

Figure8. Throughput analysis

4.5 Energy Consumption

Energy consumption of mobile nodes is ideally lower, which makes sense that the mobile nodes conserve energy. Energy consumption is inversely proportional to the lifetime of the network. The energy consumption of the proposed system is analysed and is depicted in figure 9. An extended lifetime of network serves its purpose effectively and thus, cost effective. The lifetime of the proposed work is maximized by the incorporation of clustering concepts and efficient routing. The efficiency of the system reduces the energy consumption, which results in the enhanced lifetime of the network. Chief node selected with maximum energy each time which runs network longer time.

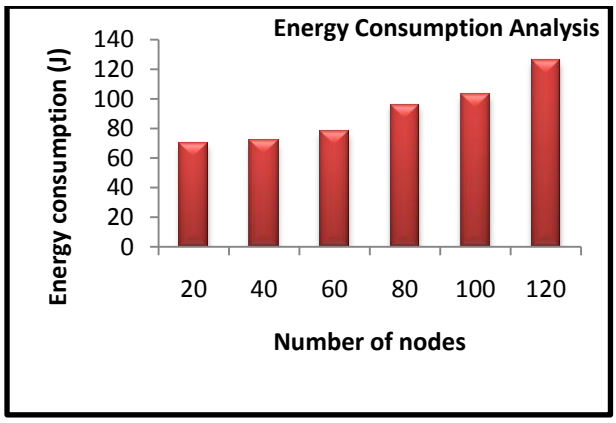

Figure9. Energy consumption analysis

From the experimental results, it is evident that the proposed work proves its efficacy with lesser delay, energy consumption and packet drop ratio. On the other hand, greater packet delivery ratio, detection accuracy, throughput and network lifetime.

5. CONCLUSION

This paper proposes an energy aware security technique that can weed out misbehaving nodes from the network. This is achieved by the incorporation of clustering technique, which saves energy. Apart from this, the chief node manages the activities of its constituent nodes and controls them. The chief node selection and the route establishment of this work are based on trust. The trust parameters are carefully selected, such that the performance of the system is enhanced and network lifetime increases. The proposed work is proved to resilient against replay and sybil attacks. The main advantages of this work are reduced energy consumption, trustworthy routing, resilient against replay and sybil attacks. In future, this work can be enhanced by focussing on some more attacks and the computational overhead can further be minimized.

6. REFERENCES

[1] S. Gwalani, K. Srinivasan, G. Vigna, E. M. Beding-Royer, and R. Kemmerer. An intrusion detection tool for AODV-based ad hoc wireless networks. In proc. of the IEEE Computer Security Applications Conference (CSAC), 2004.

[2] T. Anantvalee and J. Wu. A survey on intrusion detection in mobile ad hoc networks. Wireless/Mobile Network Security, 2006.

[3] Y. Hu, A. Perrig, and D. B. Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks. In proc. of the ACM International Conference on Mobile Computing and Networking (MOBICOM), 2002.

[4] P. Ning and K. Sun. How to misuse AODV: A case study of insider attacks against mobile ad-hoc routing protocols. In proc. of the IEEE Information Assurance Workshop, 2003.

[5] Y. Huang and W. Lee. A cooperative intrusion detection system for ad hoc networks. In proc. of the ACM Workshop on Security of Ad Hoc and Sensor Networks, 2003.

[6] O. Kachirski and R. Guha. Efficient intrusion detection using multiple sensors in wireless ad hoc networks. In proc. of the IEEE Hawaii International Conference on System Sciences (HICSS), 2003.

[7] L. Ramachandran, M. Kapoor, A. Sarkar and A. Aggarwal, "Clustering Algorithms for Wireless Ad Hoc Networks," In Proceeding: Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications, Boston, 2000, pp. 54-63.

[8] A.Ephremides, J. E. Wieselthier and D.J. Baker. "A Design Concept for Reliable Mobile Radio Networks with Frequency Hopping Signaling,"IEEE, 1987, pp. 56-73.

[9] M. Gerla and J.T. Tsai. "Multicluster, Mobile, Multimedia Radio Network. Wireless Networks," 1995.

[10] [10] S. Basagni, "Distributed clustering for ad hoc networks," 1999.

[11] M. Chatterjee, S.K. Das, D. Turgut, "WCA: A Weighted Clustering Algorithm for Mobile Ad Hoc Networks," Vol.5, No. 2, 2002, pp. 193-204.

[12] W. Choi, M. Woo, "A Distributed Weighted Clustering Algorithm for Mobile Ad Hoc Networks," Advanced International Conference on Telecommunications, 2006.

[13] C. R. Lin and M. Gerla., "Adaptive Clustering for Mobile Wireless Networks," IEEE Journal on Selected Areas in Communications, Vol. 15, No. 7, 1997, pp.1265-1275.

[14] A. Ramalingam, S. Subramani and k. Perumalsamy., "Associativity-based Cluster Formation and Cluster Management in Ad Hoc Networks," HiPC, 2002.

[15] Chen Y.Z.P. and Liestman A.L., "Approximating Minimum Size Weakly-Connected Dominating Sets for Clustering Mobile Ad Hoc Networks, 3rd International Symposium on Mobile Ad Hoc Networks and Computing, pp. 165-172, 2002.

[16] Julisch K., "Clustering Intrusion Detection to Support Root Cause Analysis", ACM Transactions on Information and System Security, Vol.6, No.4, pp:443-471,2003.

[17] Nikulin V., "Weighted Threshold based Clustering for Intrusion Detection Systems", International Journal of Computational Intelligence and Applications, Vol. 6, No. 1, pp. 1-19, 2006.

[18] Luo, M., Li, X. and Xie, S., "An Intrusion Detection Research based on Spectral Clustering", 4th International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM' 08, pp: 1-4, 2008.

[19] Jianliang M., Haikun S., Ling B., "The application on intrusion detection based on K-means cluster algorithm", International Forum on Information Technology and Applications, IFITA '09, Vol.1, pp: 150-152, 2009.

[20] Aiguo Chen, Guoai Xu, Yixian Yang, "A Cluster-Based Trust Model for Mobile Ad Hoc Networks", 4th International Conference on Wireless Communications, Networking and Mobile Computing, pp. 1-4, 2008.

[21] Feng Li, Ju Wu, "Uncertainty Modelling and Reduction in Manets", IEEE Transactions on Mobile Computing, Vol.9, No.7, pp.1035-1048, 2010.

[22] Serique, L.F.S. and De Sousa, R.T., "Evaluating Trust in Ad hoc Network Routing by Induction of Decision Trees", IEEE Latin America Transactions, Vol. 10, No. 1, pp.1332-1343, 2012.

.