Security Enhancement and Certificate Revocation in MANET using Position and Energy based Monitoring

Karpura Dheepan
Department of Computer Science and Engineering, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, India

Abstract: *Mobile Ad-hoc Network (MANET) has an advantage over their mobility and ease of deployment but it is vulnerable to various attacks to degrade the security in the network. Using cluster based certificate revocation with combination of both voting and non-voting based mechanism, attacker's certificate is revocated. But this mechanism is vulnerable to the detection of false accusation in quicker time and attacks related to high energy consumption like stretch and carousel attack. To overcome this issue and to enhance the security, Cluster based scheme along with position and energy based monitoring is proposed to revocate the certificate of the attacker node by the Cluster Authority (CA) node. Guaranteed secure network services and low energy consumption of 9% and 13% is obtained after avoiding stretch and carousel attacks respectively. It increases the Quality of Service (QoS) and reduces the packet loss in the network.*

Keywords: *MANET, cluster formation, certificate revocation, false accusation, position monitoring, energy monitoring.*

Received June 7, 2015; accepted September 20, 2015

1. Introduction

Since Mobile Ad-hoc Network (MANETs) has the advantage over mobility, ease of deployment and multi hop communication to transfer the packets from one node to another, it is preferred than any other network. Security is the important factor to be considered in MANET because it is an infrastructure less network where nodes can join and leave the network independently in Buttyan and Hubaux [4]. To degrade the security malicious and attacker nodes take part in the network to collapse the network performance and using the resource data illegally respectively in Mohammed and Abdullah [17]. Certificate management is the major mechanism used to provide secure network.

This certificate management consists of following action: protection, identification and certificate revocation which is proposed by Ayyasamy and Subramani [3]. Cluster Authority (CA) is the node which is having highest priority in the network that can able to provide the certificate to the node at the time of joining and revocate the certificate of the attacker node while leaving the network. In the certificate revocation process, the misbehaved nodes are enlisted by the votes from the neighbor node by single hop monitoring to CA and the particular nodes leads to certificate revocation by CA in Crepeau and Davis [6]. The list of misbehaving nodes is made to broadcast to the entire network. So, the misbehaving nodes cannot take part in the network activities.

Cluster Head (CH) should play a vital role in gatheringinformation regarding the absolute misbehaving nodes in each cluster. This information helps to remove falsely accused node in the list and made to take part in the network activities in Kong *et al*. [13] This certificate revocation process provides increase in reliability of the network by avoiding false accusation and secured network.

To enhance the security by avoiding false accusation effectively, position based monitoring is incorporated in Jadoon *et al*. [9]. In this monitoring, CA plays a major role in avoiding false accusation. The nodes after the deployment, each node updates its position coordinates to CA periodically. CA maintains this information as a complete database. When any malicious node comes into network and makes any false accusation, the intrusion of malicious node and its position coordinates will not be registered to CA in Zhou *et al*. [25]. So the updated database does not contain the malicious node position coordinates when comparing to the existing database maintained by CA. Hence, the CA detects the intrusion of malicious node after the comparison of database and removes the malicious node from the network in Ganapathy *et al*. [8].

Considering other energy based attacks like stretch and carousel attack, which are not discussed in the existing system are avoided by energy based monitoring along with Medium Access Control (MAC) protocol. Carousel attack is an attack in which attacker node sends packets in continuous loops composing packets with purposely introduced routing

loops. Single packet will be repeatedly passed through the same set of between the source and the destination in the network. So the energy consumption of the particular nodes in the loops will be high and the network lifetime gets decreased. Stretch attack targets the source routing in which the attacker nodes form artificially long routes, potentially passing very node in the longest path between source and the destination in the network. It increases packet path lengths, causing packets to be carried by a large number of nodes instead of using the shortest path between the attacker and packet destination. So the consumption of energy by the nodes will be higher in the longest path. And hence, the network lifetime gets degraded since many nodes get participated in the long route.

2. Literature Survey

Many certificate revocation schemes have been proposed to improve the security of the network in the literature. By this literature, the certificate revocation technique falls into two categories. They are voting and non-voting based mechanism.

2.1. Schemes Related to Voting based Mechanism

The scheme URSA: Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks [15] proposed by Luo is based on voting based mechanism. In this scheme, the certificates are provided to nodes at the time of joining the network by its neighbors. It does not contain any CA. Single hop monitoring is performed by each node and the monitored information about misbehaving nodes is exchanged with its neighbor nodes as vote. When the number of negative votes crosses the threshold value, then the certificate of the misbehaving nodes are revoked and made not to take part in network activities. When the threshold value is larger than the network degree, attacker's certificate cannot be revoked. This scheme does not consider avoiding false accusation.

A localized certificate revocation scheme proposed by Arboit [2] is also based on voting based mechanism. In this scheme, each and every node in the network takes part in the voting process. CA is present in this scheme. Each node votes with variable weights after monitoring the behavior of its neighbor nodes.

These weights are calculated according to reliability of the node by it behavior. When the weight is greater, the reliability is good in Kalpana and Punithavalli [10]. When the sum of weights in votes against the particular node exceeds the threshold value, then that particular node's certificate will be revoked. Overhead occurs because of exchanging the voting information by every node in the network that causes heavy traffic and also increases revocation time as well.

2.2. Schemes Related to Non-Voting based Mechanism

"Suicide for the common good" scheme proposed by Clulow and Moore [5] makes cluster revocation through single accusation. Providing the certificates to newly joined nodes and certificate revocation are done by CA. The certificates of both accused and accusing node will be revoked by CA. The accusing node will sacrifice itself in order to revocate the attacker's certificate. This process minimizes the certificate revocation time and overhead for cancelling the certificate of the misbehaving node. It has disadvantage of not considering the false accusation and decreases the network performance by losing the legitimate node.

Cluster based certificate revocation scheme proposed by Park *et al*. [21], where the nodes are organized into clusters. The CA maintains the Warn List (WL) and Blacklist (BL) that contains the accusing and accused nodes respectively. When the votes against a particular node exceed the threshold value after monitoring, then the accused node will be moved to BL and its certificate is revoked by the CA. Improved reliability is attained but accuracy in revocating the exact malicious node certificate and recovering the falsely accused legitimate node is slightly difficult.

2.3. Combined Mechanism

Cluster Based Certificate Revocation with Vindication Capability (CCRVC) scheme proposed by Liu *et al*. [14], where the nodes are grouped into cluster. This scheme uses both the voting and non-voting based mechanism.

So it results in less overhead, less certificate revocation time of a malicious user, high accuracy in detecting the absolute attacker in the network. By having both the mechanism in a scheme, it results in enhancement of the security in Zapata and Asokan [24]. But the technique used for the detection of falsely accused node is quite difficult and consumes time which leads to degradation in reliability.

2.4. Schemes Related to Energy based Attacks

A light weight PLGP based method for mitigating vampire attacks in Wireless Sensor Networks proposed by Farzana and Babu [7], where deployment of sensor nodes in an environment makes it vulnerable to energy based attacks because it is complex to recharge or replace the battery power of sensor nodes. There is a class of energy consumption attack called vampire attack which permanently disables the whole network by quickly draining nodes energy. In this scheme, forwarding as well as discovery phase of the protocol is done to avoid this issue. By this approach, overhead is reduced.

3. Enhanced Scheme for Cluster based Certificate Revocation

In this scheme, all nodes while joining the network will be received certificate from the CA. The certificate revocation of a misbehaving node is done quickly by only one accusation from the valid neighbor node and false accusation is minimized as low as possible with minimal revocation time.

3.1. Cluster Formation

It is difficult to detect the misbehaving node, when the nodes are deployed and randomly distributed. To overcome this issue, the cluster formation technique [14] is used. In this technique, each cluster consists of CH and the remaining nodes are called as member nodes. The nodes with fixed transmission range, the CH broadcast packets to its neighbor nodes in Pathan *et al*. [22]. The nodes that send the response message to CH through single hop are made as single cluster while the other node with dual hop or multi hop response forms the other clusters with the access of mobility. The cluster members are meant to keep on updating the information to CH in time $T_v$regarding the monitoring made within the cluster.

3.2. Importance of Cluster Authority

The CA is a node that has the highest priority among all other nodes in the network. It has the function of both providing and revocating the certificate of a node.CA also maintains two lists: WL and BL. These lists contain the list of accusing and accused nodes respectively. It also updates the WL and BL through the information obtained from each nodes. It makes use of threshold mechanism to detect the attacker in the network in Yi *et al*. [23]. When the number of votes about the node exceeds the threshold value, then the particular node is detected as the malicious node by the CA.

After detecting the misbehaving node, CA broadcasts the WL and BL to the entire network to provide the information of revocating the particular malicious node's certificate.

3.3. Process of Voting

Voting process begins with the single hop monitoring by each and every node in the cluster. Each node monitors its neighbor nodes and provides the information to CA. The CH also takes part in the voting process and polls its vote to the CA about the misbehaving node in the network. This voting process is carried in each cluster in time T_v, which is the time to cast vote by the valid nodes in the network.

3.4. Avoiding False Accusation

False accusation is made by the malicious node to the CA against the legitimate node, accuracy and performance is decreased. The legitimate node's certificate will be revoked mistakenly by the CA. To overcome this issue, the CH is meant to be active in every cluster when false accusation occurs. The CH in every cluster monitors its members and it knows whether the attack is held or not in the network. CH also maintains WL and BL containing the accusing and accused node respectively.

Firstly, after the voting process in time T_v, the CA distributes its WL and BL to all the nodes in the network. If CH does not detect any attack from that particular accused node, it identifies the presence of false accusation and it takes effort to recover its falsely accused cluster member. The CH compares the WL and BL maintained by the CA and it detects the false accused node in the BL. It requests the CA to release the falsely accused node which is listed in BL maintained by CA. CH recovers the falsely accused node by sending the recovery request of that particular falsely accused node to CA. The CA removes the falsely accused node from the BL and regains its identity to take part in the network activities. The working process of avoiding false accusation is given in Figure 1.

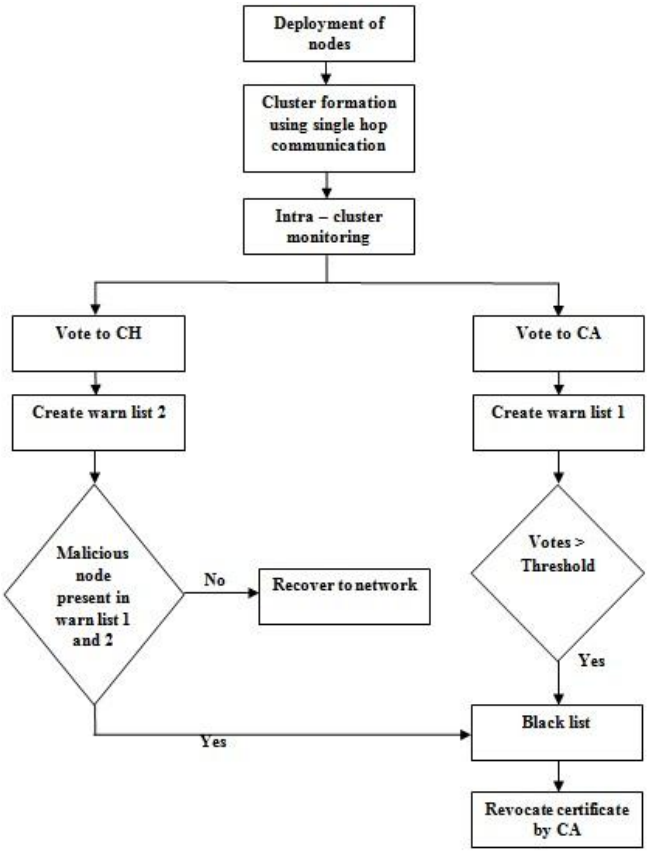

Figure 1. Avoiding false accusation.

3.5. Position based Monitoring

In MANET, each and every node has its own coordinates mentioning its position in the network range Mauve *et al*. [16]. To enhance the security by avoiding false accusation, position based monitoring can be used effectively that would provide better accuracy than the existing system. In this monitoring, geographical location of the nodes is essential to detect the situation of false accusation.

Displacement of nodes can be calculated by Equation (1).

$$D = \sqrt{(X_2 - X_1)^2 + (Y_2 - Y_1)^2} \quad (1)$$

Where,

- X_1 and X_2 are the initial and final position *X*-axis of the node
- Y_1 and Y_2 are the initial and final position *Y*-axis of the node.

In this scheme, CA plays a major role in taking action against false accusation. The nodes after the deployment in the network, each node updates its initial position coordinates to CA periodically. CA maintains this information as a complete database.

When any malicious node comes into network and makes any false accusation against the node, the intrusion of malicious node and its position coordinates will not be registered to CA in Khan *et al*. [12]. So the updated database maintained by CA does not contain the malicious node position coordinate while comparing to the existing database maintained by CA. Hence, the CA detects the intrusion of malicious node after the comparison of database and removes the malicious node from the network.

3.6. Energy based Monitoring

The existing mechanism is vulnerable to attacks related to high energy consumption in Newsome *et al*. [19]. While incorporating energy based monitoring, two types of attack are considered. They are stretch and carousel attack. These attacks are explained in detail below.

- *Carousel Attack.* Carousel attack is an attack in which attacker node sends packets in continuous loops composing packets with purposely introduced routing loops. Single packet will be repeatedly passed through the same set of nodes between the source and the destination in the network. So the energy consumption of the particular nodes in the loops will be highly consumed and the network lifetime gets decreased in Al-Jaroodi [1].

Figure 2 shows that the legitimate node takes honest route and would exit the loop immediately from node E to Sink, but a malicious packet makes its way around the loop twice or more before exiting the loop in Mohammed and Abdullah [18]. By using the repeated path, high energy consumption occurs in excess nodes in the loop leading to decrease in network lifetime.

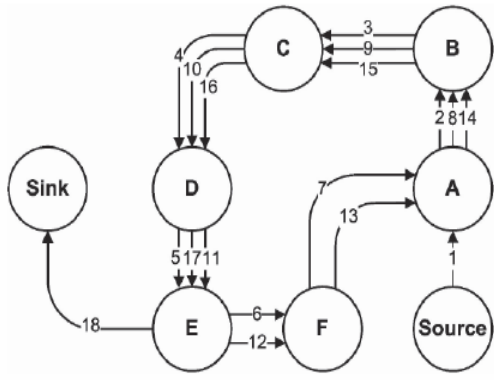

Figure 2. Carousel attack.

- *Stretch Attack.* Stretch attack targets the source routing in which the attacker nodes form artificially long routes, potentially passing every node in the longest path between source and the destination in the network. It increases packet path lengths, causing packets to be carried by a large number of nodes instead of using the shortest path between the attacker and packet destination. So the consumption of energy by the nodes will be higher in the longest path. And hence, the network lifetime gets degraded since many nodes get participated in the long route.

Figure 3 shows that the thick line is the honest route path to sink and dotted lines indicates the longest route used by the malicious node [7]. By using the longest path, high energy consumption occurs in excess nodes in the longest route and hence the network lifetime decreases.

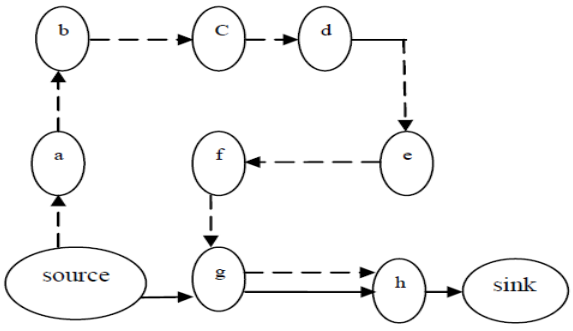

Figure 3. Stretch attack.

- *Sleep and Awake Protocol.* To minimize these above attacks, sleep and wake concept from MAC is used. By using this concept, only the shortest path nodes which are below the threshold energy are kept at wake mode and rest of the nodes are kept at sleep mode. So that packets can be routed through only in shortest path and hence the stretch attack can be rectified in Kef *et al*. [11].

The threshold energy of the nodes to be kept awaken can be calculated by Equation (3).

$$Network\ lifetime = \frac{Threshold\ energy}{Network\ energy\ consumption} \quad (2)$$

$$Threshold\ energy = Network\ lifetime \times energy\ consumption \quad (3)$$

The energy consumed after the stretch and carousel attacks and after avoiding attacks can be calculated by Equation (4).

$$Energy\ consumed = \frac{Initial\ energy - Final\ energy}{Initial\ energy} \quad (4)$$

To minimize the carousel attack, minimal number of nodes below the threshold energy in each loop is made to be in wake mode and rest of nodes to be in sleep mode. So, packets can be forwarded through the awaken nodes in each loop and hence high energy consumption of excess nodes can be reduced.

4. Simulation Results and Analysis

The above schemes are simulated in Network Simulator-2 (NS2). In this simulation, the nodes are deployed randomly. The limitation of transmission range of the node is extended by the multi-hop communication.

4.1. Cluster Formation

Nodes are deployed randomly in the terrain range of 670x670m. To form the clusters, the CH is made to broadcast packets to its neighbor nodes. The nodes which send response in single hop are considered as a single cluster. The nodes which send the response in multi-hop forms the other clusters within its transmission range. So the monitoring process to detect misbehaving node in any cluster can be found easily in [26].

Table 1. Scenario specification.

Parameters	Values
Channel Type	Wireless Channel
Propagation Model	Two Ray Ground Model
Routing Protocol	AODV
Number of Nodes	50
Transmission Range	250m
Mobility model	Random waypoint
Antenna	Omni Antenna
Simulation Time	80sec
Wireless model	1EEE 802.11
Frequency	2.4 GHz
Terrain dimension	670 x 670m
Voting time period, T_V	10s
Cluster update interval, T_u	20s
Node energy	100J

4.2. Monitoring and Voting Process

After the cluster formation, each node in the cluster monitors its neighbor node and votes to the CA which one is the misbehaving node. The CH in each cluster will monitor its cluster members and will be aware of attack made by the node in the cluster and keep on updating the status of the cluster members to the CA.

So there will be a regular link between the CH and the cluster members of the cluster. This process of monitoring and voting is followed in every cluster in the network.

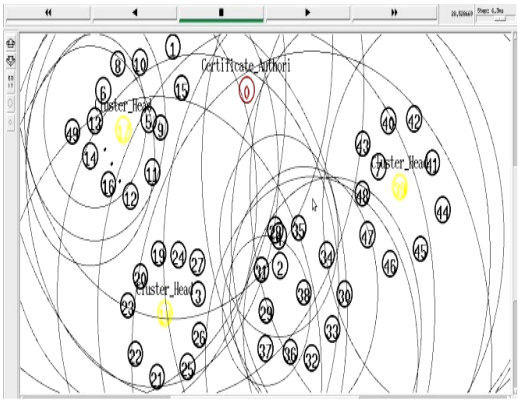

Figure 4. Broadcast starts with voting based mechanism.

4.3. Certificate Revocation

The node which polls the vote to CA is called accusing node and the node which is misbehaved is called the accused node. Since the CA has the threshold based mechanism, the threshold value is calculated as discussed earlier depending on the network degree.

When the number of votes against the accused node exceeds the threshold value, it moves the corresponding accused node to the BL. Later the nodes in the BL are lead to certificate revocation by the CA.

The WL maintained by the CA is generated once running the scenario which is displayed as run time file as shown in Table 2.

Table 2. Warn list of CA showing accusing and accused nodes.

Accusing node	Accused node
Node 11	Node 15
Node 9	Node 15
Node 1	Node 15
Node 28	Node 31
Node 4	Node 31
Node 2	Node 31
Node 15	Node 45
Node 31	Node 45
Node 5	Node 45

From this Table 2, node 15 and 31 is accused by the other nodes in the respective cluster. These nodes meet the threshold value and hence it is moved to the BL.

Thus the nodes 15 and 31 in the BL are detected as the attacker node. The certificate revocation for the respective nodes is carried out by the CA. After revocating the certificate, the attacker nodes is removed and it is made not to take part in the network activities as shown in Figure 5.

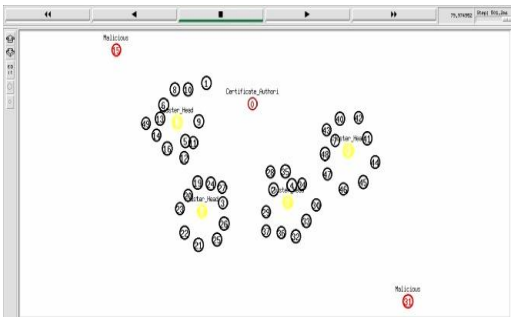

Figure 5. Removal of detected malicious user from network range.

4.4. Avoiding False Accusation

False accusation is the situation where the malicious node accuses the legitimate node falsely in order to decrease the network security.

The above Table 2 shows the WL maintained by the CA in which the nodes 15 and 31 are detected as the attacker node and in turn it accuses node 45 as the attacker node. Now, node 45 is the falsely accused node by the malicious nodes 15 and 31. This information is updated to every cluster members and CH in all clusters. The CH in every cluster maintains separate WL, BL and it is aware of attackers within its cluster. The WL and BL maintained by CA is updated to the CH, if the accused node in the BL of CA is not found in the list of CH, then the CH sends the recovery request to CA. When single request receives from CH, the CA releases the falsely accused node 45 from the BL. Node 45 is recovered by CH to take part in the network activities. Then the CA broadcasts its WL and BL to all nodes in the network regarding the certificate revocation of the malicious nodes. Considering the packet loss by Equation (5) each node, we can able to detect the absolute malicious node in the network.

$$\textit{Packet drop} = \textit{Number of packets sent} - \textit{Number of packets received} \quad (5)$$

The packet loss by each node in a cluster is given in the below graph Figure 6.

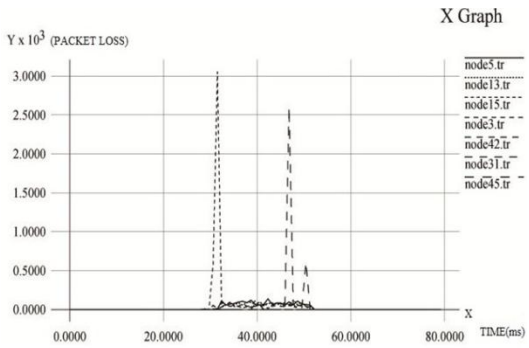

Figure 6. Packet drop analysis of nodes in the cluster.

From the Table, the falsely accused node 45 can be seen that it does not loss packets. Therefore node 45 is not an attacker node. So the nodes 15 and 31 are removed from the network by CA and makes sure that it does not take part in the network activities. Thereby it increases the reliability and accuracy with better performance than any other scheme used for certificate revocation of a malicious node in a network.

4.5. Position based Monitoring

Nodes are deployed in the cluster scheme using single hop communication same as the procedure done in the existing system. Each node's initial position is reported to the CA. And the CA maintains this position information as a database which is generated as the run time file after the simulation.

The Figure 7 depicts the intrusion of attacker node in the network. Here nodes 9, 26 and 49 are the malicious node entering the network to degrade the performance of the network.

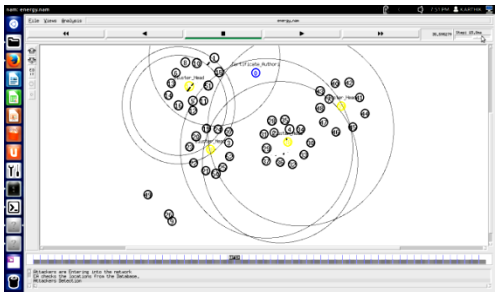

Figure 7. Intrusion of attacker node in the network.

For a specific time interval, each node updates its position information to the CA. The final position of every node in the network after the simulation time which is maintained as database by the CA and it is generated as run time file.

By comparing the initial and final position database maintained by CA, we can able to detect the intrusion of attacker or malicious node. In this scenario, the initial position of nodes 9, 26 and 49 are not found in the initial database. But these nodes intruded as the malicious node to collapse the network function and to make the false accusation of the legitimate node.

These nodes position is detected by CA while its activity in the network which its position can be found in final database maintained by CA. Hence the CA detects the presence of malicious nodes 9, 26 and 49 and leads to certificate revocation by CA and removed from the network range as shown in Figure 8.

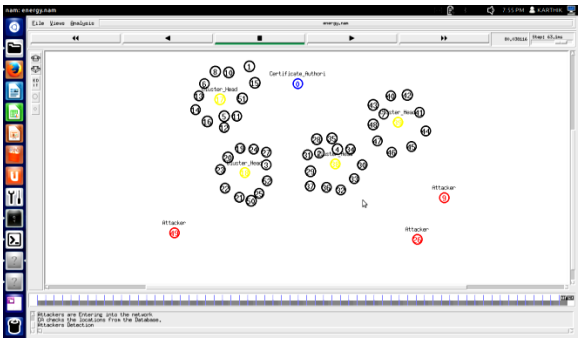

Figure 8. Certificate revocation and removal of attacker node from network.

4.6. Energy based Monitoring

Energy based monitoring is done to overcome stretch and carousel attack. These attacks lead to high energy consumption of nodes and decreases the network lifetime. To avoid these types of attacks, sleep and wake protocol is used. So the low energy consumption routing can be made.

The Figure 9 depicts the presence of stretch attack where it takes the longest path routing between source and destination and leads to high energy consumption of nodes in longest path.

By using Adhoc On-demand Distance Vector (AODV) routing protocol in Omer and Lobiyal [20], it is possible to find the shortest path between the source and the destination nodes. In this scenario, node 8 and 42 are the source and destination nodes respectively.

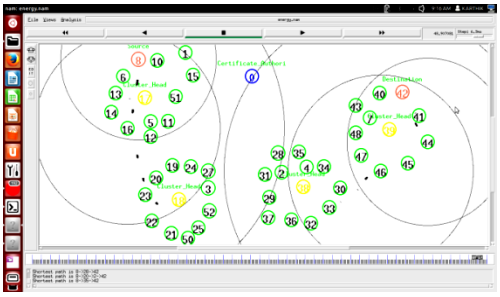

Figure 9. Occurrence of stretch attack.

When using this AODV routing protocol, the shortest path found for this scenario is nodes 8, 0, 43 and 42. Figures 10 and 11 shows the data forwarded through the shortest path indicating that the shortest path nodes having the energy below the threshold energy calculated are made as awaken node and rest of the nodes are said to be kept in sleep mode.

Using Equation (3) the threshold energy is calculated for stretch attack scenario and it is as follows

- $Threshold\ Energy = 9.421\times10^{-3}\times9.44632\,J = 89\,J$

Nodes which are below 89J are awakening nodes and others are sleep nodes and the network lifetime is determined from the simulation trace file. And hence shortest path routing is achieved when sleep and awake protocol is used. By this technique, high energy consumption of nodes in the network can be reduced and lifetime of the network can be increased.

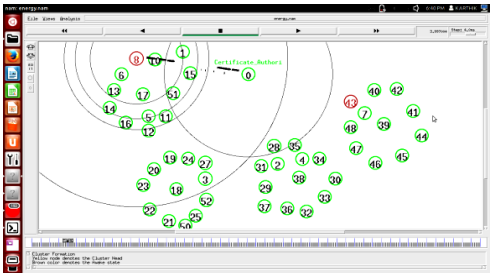

Figure 10. Data forwarding through awaken nodes in shortest path from source.

Figure 10 shows the data received in destination node by using the shortest path routing through awaken nodes 8,0,43 and 42.

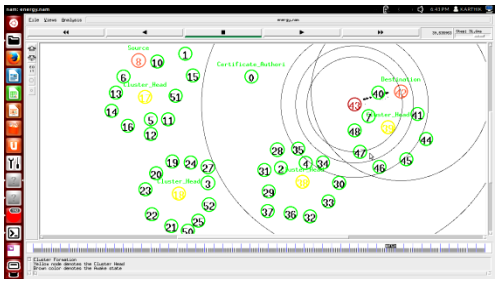

Figure 11. Data forwarding trough awaken nodes in shortest path received in destination node.

The Figure 11 depicts the graph of sleep and awake nodes in the network. From this graph, the nodes 0, 8, 42 and 43 are resulted in energy consumption indicating these nodes in the awaken mode of the shortest path and the rest of nodes in the sleep mode.

Table 3 lists the residual energy of the awaken nodes which is generated as the run time file after the simulation is completed.

Table 3. Residual energy of awaken nodes in avoiding stretch attack.

Nodes	Residual Energy
0	79.481568
8	84.928463
43	85.59822

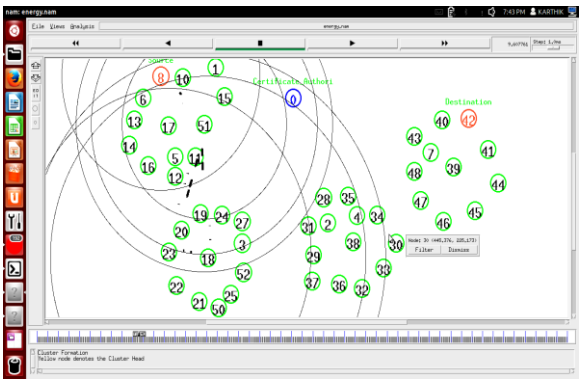

Figure 12. Occurrence of carousel attack.

The Figure 12 depicts the presence of carousel attack where it takes the continuous loop formation between the source and the destination node. By this attack, the same packet is received and forwarded from the same set of nodes. This leads to high energy consumption of many nodes in the network.

To overcome this attack, sleep and await protocol is used to minimize high energy consumption. By this concept, the nodes having the energy below the threshold energy calculated are made as awaken node in each loop and rest nodes are said to be in sleep mode. Hence the energy consumption can be reduced by avoiding carousel attack.

Using Equation (3) the threshold energy is calculated for carousel attack scenario and it is as follows

- $Threshold\ Energy = 6.183 \times 10^{-3} \times 13.909\,J = 86\,J$

Nodes which are below 89J are awakening nodes and others are sleep nodes and the network lifetime is determined from the simulation trace file.

The below Table 4 lists the residual energy of awaken nodes in each loop after the simulation is over which is generated as the run time file.

Table 4. Residual energy of awaken nodes in avoiding carousel attack.

Nodes	Residual Energy
24	76.458942
28	79.650337
30	80.411249
48	76.371022

The Figure 13 depicts the graph dealing with energy of sleep and awake nodes in the network to rectify the carousel attack. From the graph, the low peak indicates the awaken nodes in each loop between source and destination node by applying sleep and awake protocol.

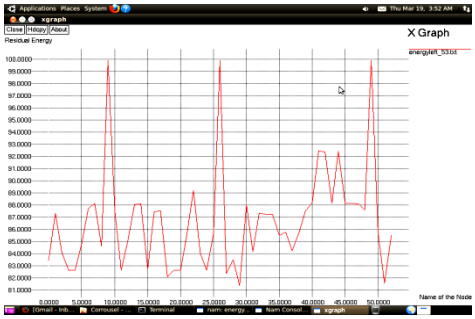

Figure 13. Energy of Sleeps and awaken nodes in the network.

Hence the high energy consumption of nodes by the carousel attack can be reduced and network lifetime can be increased by integrating the sleep and wake protocol.

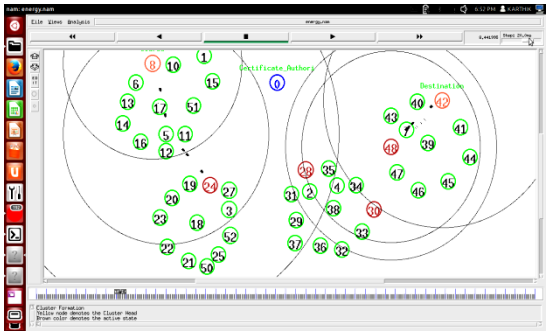

Figure 14. Data forwarding through awaken nodes to avoid carousel attack.

Figure 14 shows the data forwarding through the awaken nodes from source to destination node. In this scenario, the nodes 8 and 42 are the source and destination node respectively. The nodes 24, 28, 30, 48 denoted in color brown are the intermediate nodes and awaken nodes. And the rest of nodes are said to be in sleep mode.

Table 5 shows the network statistics dealing with residual and consumed energy of the network.

Table 5. Network statistics.

Parameters Measured	Stretch Attack	Carousel Attack
Residual Energy	4799.34 Joules	4606.20 Joules
Residual Energy (In %)	90.5537 %	86.9091 %
Actual Energy Consumed	500.655 Joules	693.816 Joules
Energy Consumed (In%)	9.44632 %	13.0909 %

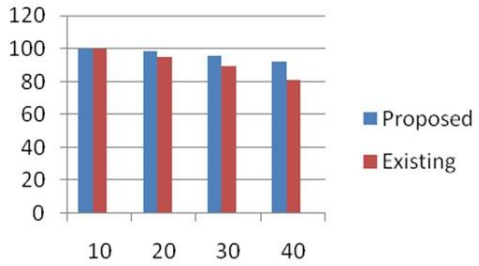

Figure 15. Analysis of Energy consumption of existing and proposed system.

The above Figure 15 depicts the energy consumption analysis of existing and proposed system. In which, the energy consumption of proposed system is lesser than the existing system and the network life time gets increased.

5. Conclusions

This work proposes a cluster-based scheme along with position and energy based monitoring to revoke malicious node certificate accurately and to solve the problem of high energy consumption due to other attacks like stretch and carousel attacks taking part in the network. This scheme can revoke the certificate of the malicious node making false accusation by the CA based on a cluster formation with position based monitoring and reduce the revocation time as compared to the existing system. High energy consumption attacks like stretch and carousel attacks are neglected using energy based monitoring integrated with sleep and wake protocol. The results have demonstrated that the proposed system guarantees the secure network without having the malicious or attacker node taking part in the network and also improves QoS with less communication overhead. The network lifetime is prolonged by reducing energy consumption about 9% and 13% after avoiding stretch and carousel attack respectively. The residual energy of awaken nodes are 82.6% and 78.3% when compared to the existing system where the energy consumption is high for voting and non-voting process and the network lifetime is prolonged.

References

[1] Al-Jaroodi J., "Routing Security in Open/Dynamic Mobile Ad Hoc Networks," *The International Arab Journal of Information Technology*, vol. 4, no. 1, pp. 17-26, 2007.

[2] Arboit G., Crepeau C., Davis R., and

Maheswaran M., "A Localized Certificate Revocation Scheme for Mobile Ad Hoc Networks," *Ad Hoc Network*, vol. 6, no. 1, pp. 17-31, 2008.

[3] Ayyasamy R. and Subramani P., "An Enhanced Certificate Authority Scheme for Authentication in Mobile Ad Hoc Networks," *The International Arab Journal of Information Technology*, vol. 9, no. 3, pp. 291-298, 2012.

[4] Buttyan L. and Hubaux J., "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks," *Mobile Networks and Applications*, vol. 8, no. 5, pp. 579-592, 2002.

[5] Clulow J. and Moore T., "Suicide for the Common Good: A New Strategy for Credential Revocation in Self-Organizing Systems," *ACMSIGOPS Operating Systems Review*, vol. 40, no. 3, pp. 18-21, 2006.

[6] Crepeau C. and Davis C., "A Certificate Revocation Scheme for Wireless Ad Hoc Networks," *in Proceedings of 1st ACM Workshop on Security of Ad Hoc and Sensor Networks*, Fairfax, pp. 54-61, 2003.

[7] Farzana T. and Babu A., "A Light Weight PLGP based Method for Mitigating Vampire Attacks in Wireless Sensor Networks," *International Journal of Engineering and Computer Science*, vol. 3 no. 7, pp. 6888-6895, 2014.

[8] Ganapathy S., Vijayakumar P., Yogesh P., and Kannan A., "An Intelligent CRF Based Feature Selection for Effective Intrusion Detection," *The International Arab Journal of Information Technology*, vol. 13, no. 1, pp. 44-50, 2015.

[9] Jadoon M., Madani S., Hayat K., and MahlKnecht S., "Location and Non-Location Based Ad-Hoc Routing Protocols under Various Mobility Models: A Comparative Study," *The International Arab Journal of Information Technology*, vol. 9, no. 5, pp. 418-427, 2012.

[10] Kalpana G. and Punithavalli M., "Reliable Broadcasting using Efficient Forward Node Selection for Mobile Ad Hoc Networks," *The International Arab Journal of Information Technology*, vol. 9, no. 4, pp. 299-305, 2012.

[11] Kef M., Chergui L., and Benmohammed M., "Self-Organization and Topology's Control for Mobile Ad-Hoc Networks," *The International Arab Journal of Information Technology*, vol. 8, no. 3, pp. 414-227, 2011.

[12] Khan S., Loo K., and Din Z., "Framework for Intrusion Detection in IEEE 802.11 Wireless Mesh Networks," *The International Arab Journal of Information Technology*, vol. 7, no. 4, pp. 435-440, 2010.

[13] Kong J., Hong X., Yi Y., Liu J., and Gerla M., "A Secure Ad-Hoc Routing Approach Using Localized Self-Healing Communities," *in Proceedings of 6th ACM International Symposium, Mobile Ad Hoc Networking and Computing*, New York, pp. 254-265, 2005.

[14] Liu W., Nishiyama H., Ansari N., Yang J., and Kato N., "Cluster-Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 2, pp. 239-249, 2013.

[15] Luo H., Kong J., Zerfos P., Lu S., and Zhang L., "URSA:Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks," *IEEE/ACM Transactions on Networking*, vol. 12, no. 6, pp. 1049-1063, 2004.

[16] Mauve M., Widmer J., and Hartenstein H., "A Survey on Position-Based Routing in Mobile AdHoc Networks," *IEEE Networks*, vol. 15, no. 6, pp. 30-39, 2001.

[17] Mohammed Y. and Abdullah A., "Security Mechanism for Manets," *Journal of Engineering Science and Technology*, vol. 4, no. 2, pp. 231-241, 2009.

[18] Mohammed Y. and Abdullah A., "I²MANET Security Logical Specification Framework," *The International Arab Journal of Information Technology*, vol. 9, no. 6, pp. 495-503, 2012.

[19] Newsome J., Shi E., Song D., and Perrig A., "The Sybil Attack in Sensor Network: Analysis & Defenses," *in Proceedings of 3rd International Symposium on Information Processing in Sensor Networks*, Berkeley, pp. 259-268, 2004.

[20] Omer K. and Lobiyal D., "Performance Evaluation of Location Update Scheme for MANET," *The International Arab Journal of Information Technology*, vol. 6, no. 3, pp. 274-282, 2009.

[21] Park K., Nishiyama H., Ansari N., and Kato N., "Certificate Revocation to Cope with False Accusations in Mobile Ad Hoc Networks," *in Proceedings of 71st IEEE Vehicular Technology Conferance*, Taipei, pp.16-19, 2010.

[22] Pathan A., Monowar M., Rabbi M., Alam M., and Hong C., "NAMP: Neighbor Aware Multicast Routing Protocol for Mobile Ad Hoc Networks," *The International Arab Journal of Information Technology*, vol. 5, no. 1, pp. 102-107, 2008.

[23] Yi P., Dai Z., Zhong Y., and Zhang S., "Resisting Flooding Attacks in Ad Hoc Networks," *in Proceedings of International Conference on Information Technology: Coding and Computing*, Las Vegas, pp. 657-662, 2005.

[24] Zapata M. and Asokan N., "Securing Ad Hoc Routing Protocols," *in Proceedings of ACM Workshop on Wireless Security*, Atlanta, pp. 1-10, 2002.

[25] Zhou L., Cchneider B., and VanRenesse R., "COCA: A Secure Distributed Online Certification Authority," *ACM Transactions.*

Computer Systems, vol. 20, no. 4, pp. 329-368, 2002.

[26] Zhou L. and Haas Z., "Securing Ad Hoc Networks," *IEEE Network*, vol. 13, no. 6, pp. 24-30, 1999.

Karpura Dheepan received his B.E degree in Computer Science and Engineering from Adhiyamaan College of Engineering, Hosur, Anna University, Chennai, India, in 2009 and M.E degree in Computer Science and Engineering from Sona College of Technology, Salem, Anna University, Chennai, India, in 2011. He has done his Ph.D in Information and Communication Engineering from PSG College of Technology, Coimbatore, Anna University, Chennai, India in 2017. He is now working as an assistant professor in Vel Tech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Vel Tech University, Chennai. His Current research interests are Wireless Sensor Networks, MANET, Networking and IOT.