An Intelligent Efficient Secure Routing Protocol for MANET

Shailender Gupta and Chander Kumar

YMCA Unversity of Science and Technology, India
shailender81@gmail.com-mail, nagpalckumar@rediffmail.com

Abstract

The security issues are more complex and challenging in Mobile Ad hoc Networks (MANETs) than other conventional wireless networks due to peer to peer behavior of the participating nodes, absence of centralized routers and routing through intermediate nodes. For successful communication between a pair of source and destination it is vital that the intermediate nodes be trustworthy and don't drop packets. Nodes in an ad hoc network may not be trustworthy either due to selfishness created by power loss or due to maliciousness relating to rogue intentions. A node that was earlier trust worthy may no longer be so at later stages due to loss of power making the continuous dynamic evaluation of trust a necessity. Also the security requirements may vary as per the conditions on the scenario. This paper proposes an intelligent protocol that takes care of both selfishness and maliciousness by evaluating the trust dynamically. The protocol is able to adjust the trust level requirement as per the demand of the situation and can work in various levels of insecure environments. With the help of exhaustive simulations, the performance of this protocol has been demonstrated and compared with the normal AODV protocol in standard lab environment.

Keywords: *Ad hoc network, routing, selfish, trust, security*

1. Introduction

The ad hoc networks are built and operated by the constituent wireless mobile nodes. The nodes in these networks have limited transmission range and communicate with the rest of the nodes in the network through intermediate nodes. Thus membership of such a communication network requires that the constituent nodes behave in the benevolent manner throughout the operation of the network. The nodes in these networks are mobile, leading to the dynamic topology of the network. Due to the involvement of intermediate nodes in the routing process and the dynamic topology of the network it is necessary that there should be a mechanism to find the route between a given pair of source and destination time and again. Such a mechanism is known as protocol. A protocol may be proactive or reactive [1]. In a proactive environment the routes are maintained in the tables of constituent nodes and available at all times to avoid the latency that may occur in new route discovery process. However such a mechanism requires the consistent periodic interaction between the participating nodes of the network leading to the consumption of energy even when no communication is occurring. In the reactive environment, the routes are discovered on need felt basis. Though the periodic interaction energy is saved in the reactive protocol scenario yet the latency in the route finding process is a cause of concern.

Whether the protocol is reactive or proactive, the communication between a pair of source and destination requires intermediate nodes, unless the source and destination pair is at a distance of one hop. All the participating nodes in the ad hoc network act like mobile routers [2] and have the control over the data passing through them. Therefore for the success of the ad hoc network it is vital that all the participating nodes are credible and behave in the selfless

manner. However such a behavior is very difficult to find and like all other networks the ad hoc networks are also prone to both passive and active attacks [3]. An active attack may involve fabrication or modification of the data / control packets, dropping of data / control packet or it may involve the impersonation by a malicious node [3]. A passive attack involves the snooping or eavesdropping upon the network traffic and to extract the vital information [3-6].

An ad hoc network has to be protected from two types of behavior: selfish and malicious [7]. The malicious behavior of the participating nodes is common to all sorts of communication networks wherein the rogue nodes attack the network in passive and/or active manner. However, the selfish behavior of the nodes is a problem specific to the ad hoc networks [8-10]. A selfish node is reluctant to spend its own energy for forwarding the data of other nodes of the network while assuming the faithful behavior from other nodes for itself [9, 11].

The literature on ad hoc network contains measures to deal with both selfish and malicious behavior. These measures involve employing cryptographic techniques to protect the data from malicious nodes and using the 'tit for tat' strategy for dealing with the selfish nodes [12-16]. It was observed that the use of cryptographic techniques to protect the data is futile if the data packets are dropped by a selfish or malicious relaying node [16]. Thus between a given pair of source and destination, it is vital to choose the intermediate nodes which are trustworthy. Such a mechanism involves the development and implementation of a trust model that computes the trust worthiness of the intermediate nodes using a trust index. Many such trust models have been reported in the literature of ad hoc networks [17-28].

On the basis of their organization, the ad hoc networks can be classified into two categories: pure and managed [29-30]. In a pure environment any wireless node can join or leave the network without any prior intimation or formality [31]. In the managed ad hoc network the participating nodes need a prior registration before entering or leaving the network. The managed networks are suitable for the law enforcement and military setups where the requirements are known in priory. It takes time to setup a managed ad hoc network; in contrast to this the pure ad hoc networks can be established rapidly in spontaneous manner. It is possible to implement stringent security measures in managed ad hoc networks but the same is not true for pure ad hoc networks.

To implement a trust based protocol it is advisable to have a managed ad hoc network though it may involve the violation of the basic definition of the ad hoc network. Keeping in view the basic nature of the ad hoc network it is desirable that the managing agency doesn't interfere in the routine working of the network and keeps its involvement to the level of entry / exit registration and providing the basic guidelines of the protocol to be followed by the participating nodes as and when they enter or leave the network.

In the trust based protocols the behavior of each node in the network is observed by the other nodes of the network and a trust index is developed about the node under observation. This trust index developed by a node about other nodes of the network can either be due to its own observation (first hand trust) or may be due to the opinion given by the other nodes (second hand trust). The example protocols in this category include CONFIDANT [22], SORI [24], CORE [21], WATCH DOG and PATHRATOR [9] and OCEAN [32]. Also efforts have been made to develop trust based version of standard protocols such as AODV [29]. Literature on ad hoc network also contains a Trust Aware Routing Protocols (TARP) [33] wherein the different features of a node such as processing capability, cryptographic support, power support etc. combine to indicate its trustworthiness. These trust based protocols suffer through the following major drawbacks: Firstly, it takes time for the trust index to grow to a requisite level before a node can be selected as the intermediate node with confidence [34].

Secondly, it is quite possible that a node which was earlier trustworthy may no longer be so as it may become selfish due to its energy loss with the passage of time. Thirdly, a node supplying the second hand trust information may itself be not reliable. Fourthly, the threshold trust index requirement may be different for the different application scenarios. Thus it is necessary to have mechanisms that give

- A kick start to the system on the initial basis for the purpose of trust worthiness.
- Evaluate the trust dynamically
- Incorporate the trust worthiness of the node supplying the second hand trust information.
- Could take into consideration the various levels of security requirements while deciding the trust requirement *i.e.*, if the security considerations are stringent then the requisite trust level should be increased dynamically and vice versa.

Keeping all these aspects into consideration this paper proposes a new protocol for ad hoc networks. The protocol has been named as AODV-n. The value of n can be 0,1,2,3 depending upon the security level requirements, 0 being the least secure and 3 being the most. The normal AODV protocol has been referred to as plain AODV.

While designing this protocol it was assumed that there is a managing agency that controls the entry and exit of the nodes in the environment of the ad hoc network and provides the basic guidelines of the protocol to be followed but doesn't play any role in deciding the communication between the nodes in the network. The salient features of the protocol are as follows:

- Authentication of the trusted node on the basis of light weight cryptography for creation of the trustworthy route using challenge response mechanism. (Cryptography not used for data encryption). This authentication mechanism has also been used to provide the initial level of trust to give the kick start to the system.
- Exchange of residual power information to know about potentially selfish nodes
- Intelligent multilevel trust options based protocol to cater the different levels of security needs
- Credibility of the nodes taken into consideration while computing the second hand trust.
- Compassionate behavior for the selfish nodes in their initial stage.

The proposed protocol was implemented on the QualNet-5.0 Simulator with the technical support of Eigen Technologies. Various parameter of the network were measured under standard conditions and the performance of the network was evaluated. These results have been provided and discussed in the simulation and results section of this paper.

The rest of the paper has been organized as follows: Section 2 contains discussion on the relevant previous work. Section 3 provides a discussion on the trust model as used in designing the protocol AODV-n and its application and implementation in routing process. Section 4 discusses the simulation environment and a brief description of the results obtained. Section 5 provides an analysis of the results. This follows the concluding remarks in Section 6.

2. Literature Survey

A MANET can exist and work if and only if the participating nodes behave in a cooperative manner wherein the data packets of other nodes are faithfully forwarded. But like all other aspects of real life here also the conditions are not ideal and MANETs are vulnerable to black hole (Packet Dropping) and Gray hole (Selective forwarding) attacks [35-36] by the malicious and the selfish nodes. Keeping this aspect in consideration, the literature on ad hoc networks contains a lot of papers which provide strategies or mechanisms to deal with or cope up with such nodes. The strategies used to tackle these nodes can be categorized into two basic categories: Detect and exclude [21-22, 24, 9, 32] and motivation/ incentive based approach [37- 41, 12-13].

The Detect and exclude strategy uses a reputation based system wherein the participating nodes observe the forwarding behavior of their fellow nodes and create a reputation index about them. A node that crosses the threshold value of the reputation index is considered to be a trusted node and is eligible for forwarding the data packets. The system detects and punishes the node with low reputation by isolating them from the MANET environment.

The Watchdog and Pathrater [9] is an improvement over DSR protocol. The watchdog mechanism detects the selfish nodes using promiscuous mode and the pathrater assigns the trust index to different nodes of the network based upon the feedback received from the watchdog. The CONFIDANT [22] protocol contains a trust manager that sends an alarm to friend nodes to indicate the misbehavior observed by its monitor (similar to watchdog). The CORE [22] protocol involves the calculation of trust index based upon three kinds of observations: direct observation made by the node itself, indirect observation received from other nodes and the functional observation made during a specific task. The OCEAN [32] protocol avoids the use of indirect trust information and relies upon the own observation of the node about other nodes. The rate of growth of trust in such an environment is quite slow and it may take a lot of time for the reputation index to rise to its requisite threshold level. Moreover the first hand trust is restricted to next hop only. In an effort to increase the rate of growth of trust, Liu, *et al.*, [20] proposed to extend this first hand observation to the level of two hops. In their proposal, Dewan, *et al.*, [18] have stressed upon the source node to choose the next hop node with very high trust index.

The motivation/ incentive based approach involves the offering provision for the payment for every packet forwarding. Each node receives a payment for forwarding the data packets and makes the payment to other nodes for getting its data packets forwarded. The payments can be in the form of money, stamps, points or some virtual currency [37-41, 12-13]. In their work, Buttyan and Hubaux [12, 37] introduced a virtual currency nuglets that would be credited to the account of a node for forwarding the data packets. Crocraft, *et al.*, [39] proposed a mechanism that determines the appropriate price for forwarding in such a manner that discourages the selfish behavior in the MANET environment. However, such a system suffers from many drawbacks such as: A node may deny the service even after receiving the payment [13, 41], the service is rendered but may be of poor quality, a selfish but wealthy node is not punishable in such an environment, and a node which is cooperative but is lying in low traffic zone may not be able to get the services as it is not in a position to get enough payments [42]. Keeping all these aspects in view, the motivation/ incentive approach has been less popular compared to its detect and exclude counterpart.

In their work Ze Li and Haiying Shen [42] have proposed the need for an integrated system based upon both trust based approach and the price based approach using an analysis based upon the game theory. Both the trust based approach and the incentive based approach are expensive at their individual level both in terms of transmission overhead, data maintenance

and computational overhead. A combination of the two may lead to a very expensive environment in terms of latency, transmission overhead and data maintenance.

This paper proposes an intelligent protocol based upon detect and exclude strategy using a trust model given in the subsequent section.

3. The Trust Model

We have applied our trust model to the basic AODV protocol. The trust model performs the task of trust derivation, trust computation and trust class assignment, and the trust application. In the trust derivation stage, the nodes of the network derive the trust about the other nodes of the network on the basis of the interaction and the observation of the behavior while forwarding the data / control packet using promiscuous mode. In the trust computation and trust class assignment stage a node assigns trust class to the various nodes of the network which is a representative of their trust worthiness. In the trust application stage, the trust class of the nodes is used to derive the route between a given pair of source and destination on the basis of requisite security.

3.1. Trust Derivation

The major basis for trust derivation is the sincerity of the immediate neighbouring node in their behaviour for the packet forwarding. But as discussed earlier in the literature review section of this paper, it takes a significant amount of time for the trust to grow to the requisite threshold level before it can be used for considering a node to be really secure for selection as intermediate node [34]. To give a head start to the trust mechanism a concept of Random Electronic Code Book (RECB) has been used. The RECB contains 32 bit unique random cipher code for each possible 32 bits of plaintext information. There is no mathematical or logical relationship between the plaintext and the cipher code and the mapping between the two is one to one. The only way one can get the cipher text corresponding to a plaintext is through the matching process in RECB. Figure 1 shows the basic structure of RECB. We have used this RECB for challenge response mechanism for mutual authentication of the nodes. When the network is in the infancy stage and trust levels have not grown to the requisite level it is the initial source of trust. The advantage of using RECB is that it does not hinder the scalability of the network.

In the MANET environment, power is a critical factor and all the nodes in the network are least interested to spend their power for others unless they are motivated or have some fear for the penalty. The situation becomes more critical if a node is already deficient in power. In such a scenario it is quite possible that a node that was earlier trust worthy may no longer be so if it has spent a significant amount of power. It is therefore necessary to know if the node chosen for route creation is well off with the power. If it is not the case it may not oblige with forwarding the data for other. Such a node, though legitimate, may not show the benevolent behavior. To incorporate this aspect in the trust mechanism, the proposed protocol takes into consideration the residual power of the node being chosen for route formation. The information about residual power of the node is a part of periodic updates. This residual power in a node has been divided into four categories Low, medium, high and very high. To make a node truthful in providing its power status information, other nodes should not forward its data more than w times where w can be suitably chosen (w=5 in our case).

Therefore, while considering the trust worthiness of a node following three aspects were taken into consideration

- Possession of RECB

- Instantaneous Power Status
- Observed Behavior

The RECB is supposed to be supplied by the managing agency. Its non possession makes a node a foreign node that has joined the network without prior registration. Such a node is not considered to be a legitimate one and is not chosen for route formation.

Plain text	Random Cipher Code
0000 0000 H	BCDE 000A H
0000 0001 H	FFFF BA00 H
0000 0002 H	CC00 0143 H
0000 0003 H	ABCD 0321 H
----------	----------
----------	----------
----------	----------
FFFF FFFF H	0A0B 01FF H
H DENOTES HEXADECIMAL	

Figure 1. Structure of RECB

The information about instantaneous power status is vital as a power deficient node is very likely to be selfish. The power status information is exchanged by a node with its immediate neighboring nodes on the periodic basis. The nodes are obligated to speak truth about their power status otherwise they will stand black listed and their data will not be forwarded. The information about the power status and the possession of RECB is collected through the Trust Request and Reply Packet TREQ and TREP respectively as shown in the Figure 2 and Figure 3.

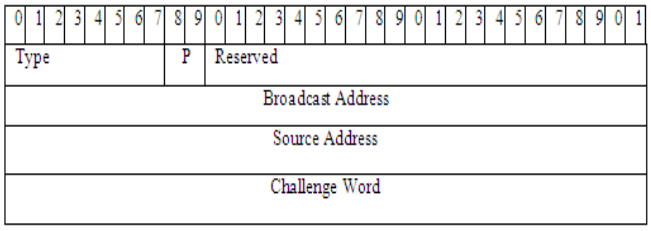

Figure 2. Format of TREQ Packet

The details of the TREQ packets are as follows:

- The Type field indicates the type of the packet, trust request packet in this case. The value assigned to this field was 0000 0101.

- The P field provides the power status of the source node. The power status field consumes two bits of information with their meaning as follows: 00 (low), 01(medium), 10 (high) and 11 (very high).
- Broadcast Address indicates the packet will be broadcast to all the nodes which are in the transmission range of source node (set to 255.255.255.255)
- Source Address indicates the address of the node which generates the TREQ packet.
- Challenge Word is of *32 bit and is used for authenticating the neighboring nodes*

Figure 3 shows the format of the TREP packet which is sent by a node to the other node to provide the trust information about the other nodes. This packet is sent in the unicast manner.

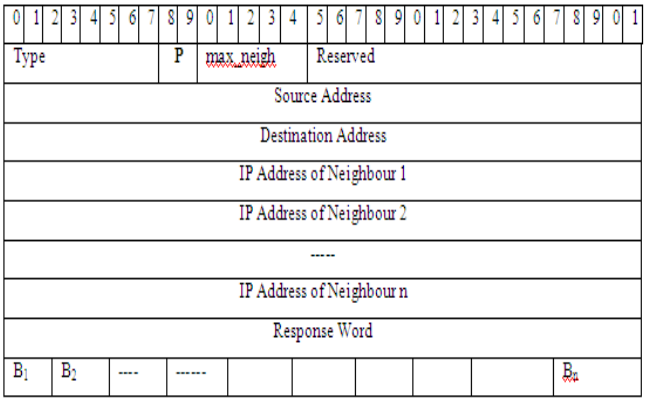

Figure 3. Format of TREP Packet

The purpose of various fields in this packet is as follows:

- The Type field indicates the type of the packet, trust reply packet in this case. The value assigned to this field was 0000 0110.
- The P field provides the power status of the replying node.
- The max_neigh field indicates about how many number of nodes the trust information is being supplied. The maximum limit set for this field was 8. The count written in this field is used by the receiver node of the TREP packet to match with the number of IP addresses of the nodes and their behavioral index.
- Source Address indicates the address of the replying node which received the TREQ packet.
- Destination Address is the address of the node which generated the TREQ packet.
- IP address of Neighbour i indicates the IP address of the ith node about which the trust information is being provided.
- Response Word is generated in response to the challenge word
- Bi is the observed behavior about the ith node

The major contributor to the trust mechanism is the observed behavior about the node under consideration. To observe this behavior of the nodes in the ad hoc network

promiscuous mode operation was used. The subsequent section talks about the trust computation mechanism on the basis of observed behavior.

3.2. Trust Computation and Trust Class Assignment

The major constituent of the trust mechanism is the observed behavior. A node X after forwarding the data/ control packet to the neighboring node Y observes the behavior of the node Y in the promiscuous mode. If node Y faithfully forwards the packets received from X then it is a positive inference P, if Y drops the packets received from X then it is a negative inference N. Both P and N are initialized to zero at the time when X encounters Y for the first time or information is received by X about Y from other node at the first time (Second Hand Trust). Our trust model uses both these aspects of the trust.

$$B_y = B_y + \frac{aP - bN}{aP + bN + K}$$

We start our discussion with first hand trust in which a node X develops trust about the other node Y on the basis of own observation. The equation for the First Hand Trust is

where

- By refers to the observed behavior index related to node Y as observed by the node X. Initial value of By is set to 0.5, making it intermediate level trust worthy. It is necessary that the node Y under consideration must possess the RECB.
- a, b and K are the constants that determines the growth of the trust. The constants a and b are the weight factors assigned to the positive and negative evidences respectively and b >> a. The constant K makes the observed behavior index asymptotic in nature due to which the trust level reaches to the level 1 at infinite time in the asymptotic manner.

Another contributor to the trust mechanism is the second hand trust. The role of second hand trust comes into play when the network is in its active stage after sometime of its deployment. Every node in the network has information (First hand Behavior) regarding its neighboring nodes received in the promiscuous mode. This information needs to be circulated to the other members so that others should know about the selfish and malicious nature of the nodes in the network. The node appends first hand behavioral index of its neighboring nodes to other nodes through the TREP packet as shown in Figure 3. Upon receiving this packet a node calculates the weighted average of all the second hand behaviors that it receives from all the neighbors but discards the second hand behavior received from blacklisted members. When a node X receives value of behavioral index about a node Y from various neighboring nodes then it computes the weighted trust average on the basis of Equation given below.

$$SHB_y = \frac{\sum_{i=1}^{N} w_i B_y}{N}$$

Where wi is the weight factor that depends upon the current trust class of the node providing the trust information and N is the number of nodes supplying the trust information about Y. Table 1 provides the list of weight factors assigned to various categories of nodes. Table 2 assigns behavioral class to a node on the basis of reputation index.

The node combines the first hand and second hand trust to calculate the overall behavioral index (Ty) according to the Equation shown below.

$$T_y = e^{-t\alpha} B_y + (1 - e^{-t\alpha}) SHB_y$$

Table 1. Weight of Trust Class

Trust Class	Weights (w_i)
Black List	0
Selfish	0.5
Trust worthy	1
High Trust worthy	1

Table 2. Rule Base to Classify the Type of Behavior

Reputation Index $\mathbf{B_y}$	Behavioral Class
Less than 0.2	Bad
0.2-0.3	Poor
0.3-0.5	Medium
0.5-0.7	Good
Above 0.7	Very good

Where t is time period elapsed since the inception of the network. It can be seen that when t is low the first hand trust over powers the second hand trust and as t increases the second hand trust starts dominating. Here α is a constant that determines the ratio of mixing the first and second hand trust. On the basis of overall trust Ty, possession of RECB and the current power status a node is classified into a particular category of trust class among the following: Blacklist, Selfish, Trustworthy and High Trustworthy. Table 3 provides the rule base for classifying a node into a particular trust class.

Table 3. Rule Base to Classify a Node into Various List

Behavior type	RECB	Power Status	Trust class
---------	No	----------	Blacklist
Bad	Yes	Low	Selfish
Bad	Yes	Medium	Blacklist
Bad	Yes	High	Blacklist
Bad	Yes	Very high	Blacklist
Poor	Yes	Low	Selfish
Poor	Yes	Medium	Selfish
Poor	Yes	High	Blacklist
Poor	Yes	Very high	Blacklist
Medium	Yes	Low	Selfish
Medium	Yes	Medium	Trust worthy
Medium	Yes	High	Trust worthy
Medium	Yes	Very high	Trust worthy
Good	Yes	Low	Trust worthy
Good	Yes	Medium	Trustworthy
Good	Yes	High	High trustworthy
Good	Yes	Very high	High trustworthy
Very Good	Yes	Low	Trust worthy
Very Good	Yes	Medium	High trustworthy
Very Good	Yes	High	High trustworthy
Very Good	Yes	Very high	High trustworthy

The trust class is given binary values that are shown in Table 4.

Table 4. Trust Class Binary Values

Trust Class	Binary values
Black list	00
Selfish	01
Trust worthy	10
High trust worthy	11

3.3 Trust Applications

This phase involves application of the computed trust class in finding the route. The Route Request Packet (RREQ) shown in the Figure 4 contains a field TC that indicates the minimum requisite qualifying class which an intermediate node should possess in order to be selected. The RREQ is sent in the form of multicast fashion to the neighboring nodes qualifying the trust class. If the source node doesn't get the route with desired trust class then it has two options either to regenerate the route request with lower trust class or go in waiting loop and regenerate the RREQ after sometime when the local scenario changes. Figure 5 and Figure 6 depict the flowcharts for route finding.

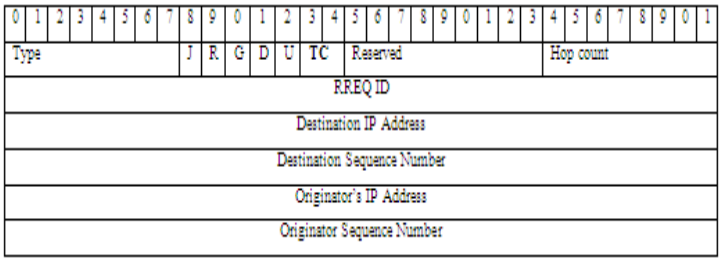

Figure 4. Modification in RREQ Packet

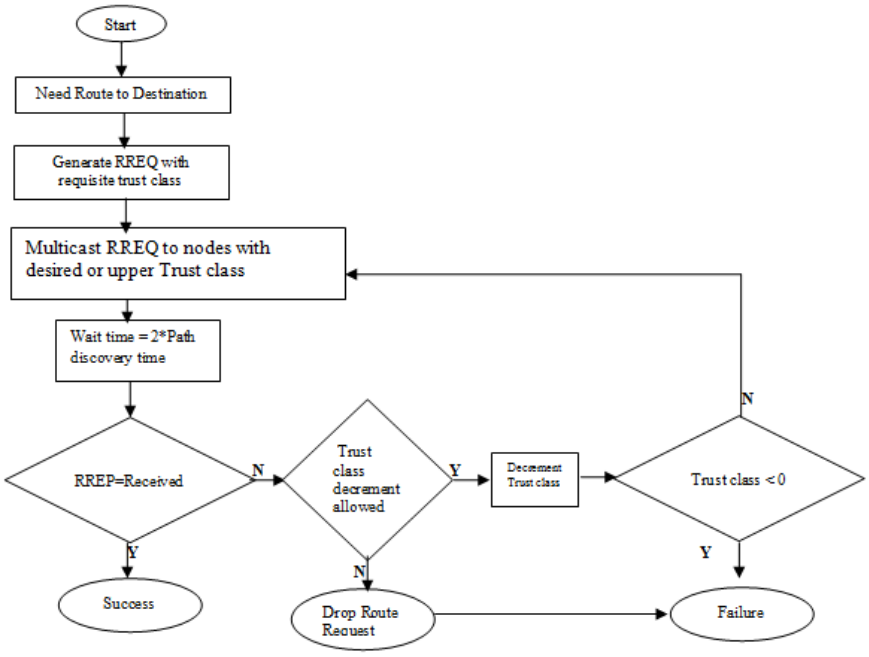

Figure 5. Route Request Phase Source Node

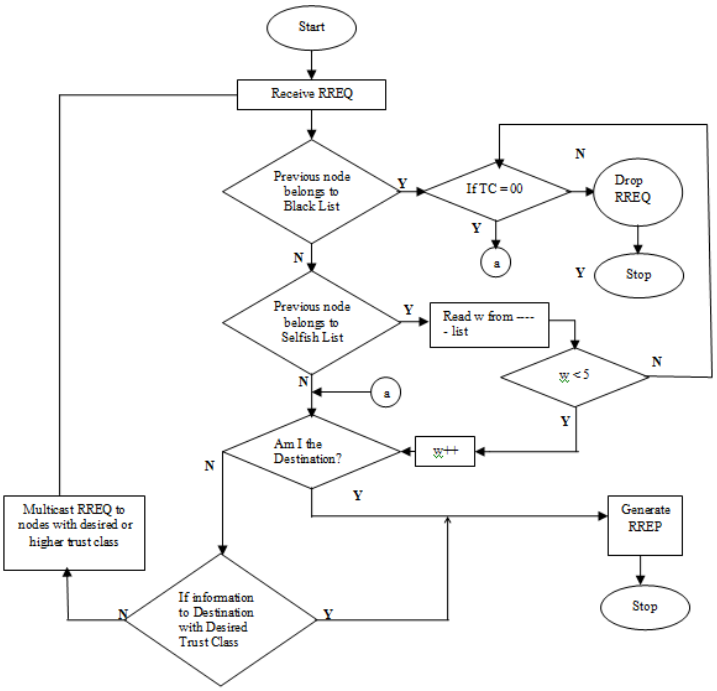

Figure 6. Route Request Phase (Intermediate node)

4. Simulation and Results

4.1. Simulation Setup

The QualNet-5.0 simulator was used to evaluate the performance of plain AODV and our protocol AODV-n under attack condition. The software provides standard simulation conditions, GUI facilities and comprehensive environment for designing the protocol. The technical support received from Eigen Technologies, New Delhi acted like a catalyst.

4.2 Parameter Chosen

The basic parameters used in the simulation process are as given in Table 5.

Table 5. Basic Simulation Parameter

Examined Protocol	AODV, AODV-n
Simulation Time	30-2000 sec
Simulation Area	1500 X 1500 sq. mt
Number of Nodes	60
Traffic Type	CBR (UDP)
Energy Model	Mica- Motes
Communication Model	IEEE 802.11
Battery Model	Linear
Data Rate	1 mbps
Pay load size	512 byte
Default Battery	1200mah
Trust update interval	1 sec
Number of malicious nodes	0-30
Number of selfish nodes	0-30

4.3 Attack Pattern

Selfish Node Attack: In this attack, a node tries to utilize the network resources for its own profit but is reluctant to spend its own for others since its residual battery power becomes very low. As the time passes in the network the chances of nodes becoming selfish gets increased.

Malicious Node Attack: In this attack, a malicious node dumps all the data packets/ Control packet which it is supposed to forward. It receives all the packets meant for it but at the same time doesn't forward the packets that are intended for others.

4.4 Assumptions

The following assumptions were made for simulation purpose:

- Each node declares its residual battery status correctly.
- The malicious node work in individual manner and there is no such group.
- The participating nodes are not in a position to modify the control packets. .

4.5 Metrics Used

To evaluate the efficacy of the proposed protocols following metrics were used:

- **Successful Route Formation:** Percentage of route formed successfully to the number of route requests generated by the source.
- **Average Hop Count:** Average number of hops for all successful route formation.
- Throughput: How fast data can pass through a network. In our simulation scenario it is the number of bits passed through the network in one second.
- **End-to-End delay:** Time taken for a packet to travel from the CBR (Constant Bit Rate) source to the destination. It is a measure of average data delay in an application involving data transmission.
- **Jitter:** Occurs when in a transmission scenario different packets take different amount of time in reaching from source to destination. Jitter can be measured by using the standard deviation of packet delay. If a communication system has large amount of jitter then the signal quality is very poor.
- **Packet delivery ratio (PDR):** Ratio of number of data packets successfully received at the destinations to the total number of data packets sent by various sources.
- **Network Lifetime:** Time at which first node of network gets dead. Or Minimum time at which all the node of the network gets dead.

4.6. Results and Discussions

4.6.1. Successful Route Formation: It was observed that percentage of successful route formation was almost same in case of plain AODV irrespective of the malicious node concentration as shown in Figure 7(a). However there was a significant drop in the successful

route formation with the increase in malicious node concentration in case of AODV-1, 2, 3. Though there was a decrease in the case of AODV-0 but this drop was small.

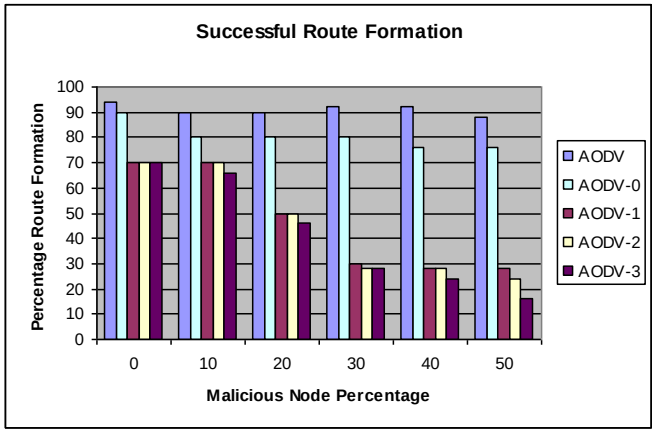

Figure 7(a). Successful Route Formation with Malicious Nodes

In case of selfish node scenario, the successful route formation was close to 100% in case of plain AODV irrespective of selfish node concentration as shown in Figure 7(b). A small drop was observed in case of AODV-0 with the increase in selfish node concentration. Though there was a decrease in the percentage of route formation in case of AODV-1, 2, 3 with the increase in selfish node concentration but this decrease was much less than in case of malicious node scenario. The underlying reason for this being the obligation to the selfish nodes to speak truth about their power status.

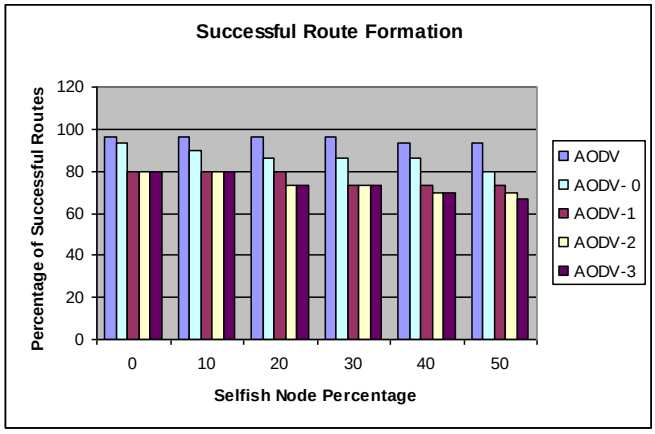

Figure 7(b). Successful Route Formation with Selfish Nodes

4.6.2 Average Hop Count: The trend in average hop count showed no change for plain AODV with the increase in malicious node concentration as shown in Figure 8(a). There was marginal increase in hop count in case of AODV-0 with the increase in malicious node concentration.

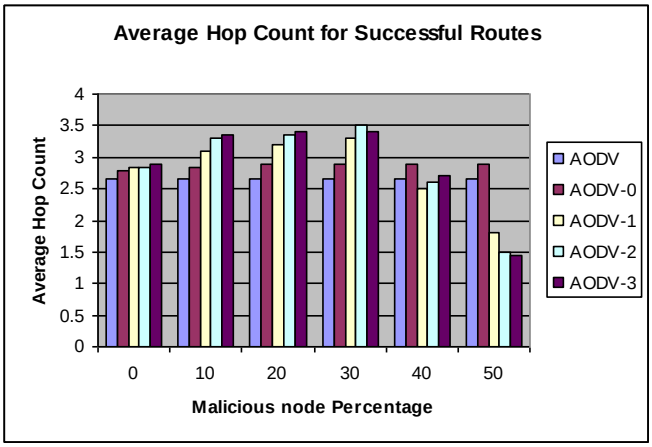

Figure 8(a). Average Hop Count for Malicious Nodes

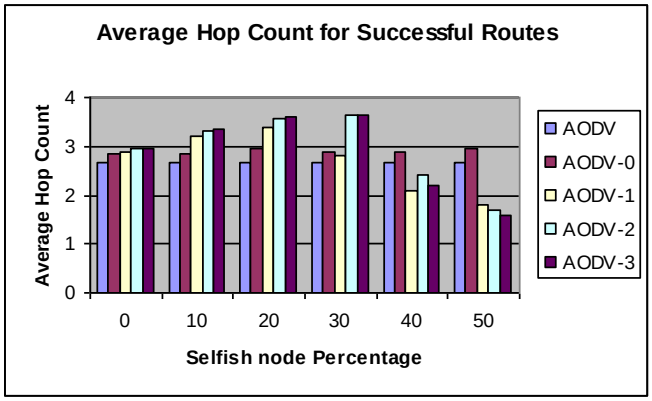

Figure 8(b). Average Hop Count for Selfish Nodes

The trend in case of AODV-1, 2, 3 showed an increase initially but a decrease later on as the malicious node concentration increased. A careful scrutiny of the scenario showed that when the malicious node concentration was very high the successful route formation was limited to immediate neighbors or their next neighbors in most of the cases. Similar results were observed in case of selfish node scenario as shown in Figure 8(b).

4.6.3. Throughput: To measure the throughput the data was sent at the rate of 4096 bits/sec. The plain AODV works well when there is no malicious or selfish node as shown in Figure 9(a). As the malicious node concentration increases the throughput of plain AODV decreases very fast and reduces to 55% as the malicious node concentration node reaches to 50%. However, the AODV-n protocol manages to resist the impact of malicious nodes and the throughput drops to the level of nearly 70%. Also it is worth noticing that when the malicious node concentration is to the level of 30 to 40%, the AODV-n protocol has the throughput to the level of nearly 85 to 90%. Since the nodes are obligated to speak truth about their current power levels in the selfish environment the throughput of the AODV-n protocol is nearly 95-100%. However, there is a significant decrease in the performance of plain AODV as shown in Figure 9(b).

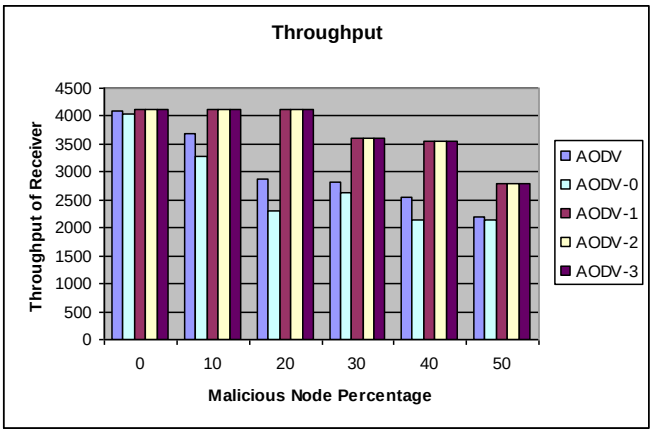

Figure 9(a). Average Throughput for Malicious Nodes

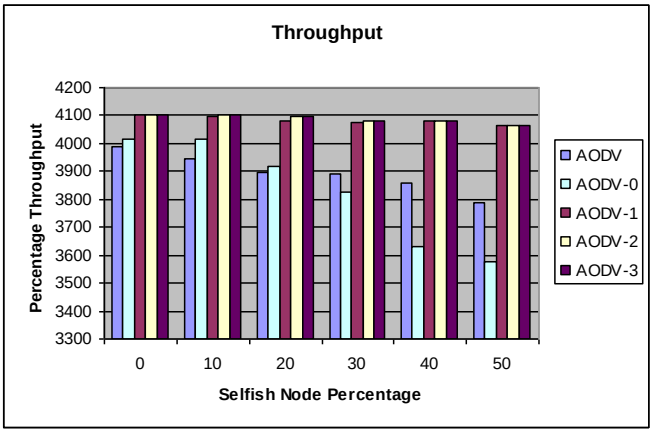

Figure 9(b). Average Throughput for Selfish Nodes

4.6.4. End to End Delay: It indicates the time taken for a packet to travel from the CBR (Constant Bit Rate) source to the destination. It represents the average data delay that an application experiences while transmitting data. At low concentration level of malicious nodes, the end to end delay is much lower in case of plain AODV and as the concentration of malicious nodes increases the average delay is much lower in case of our protocol AODV-n as shown in Figure 10(a). The performance of plain AODV and AODV-n in the selfish environment was found to be random with no consistent change in one direction, on analysis it was found that as the selfish node concentration increases most of the routes formed were of low hop count of the order of 1 or 2 as shown in Figure 10(b).

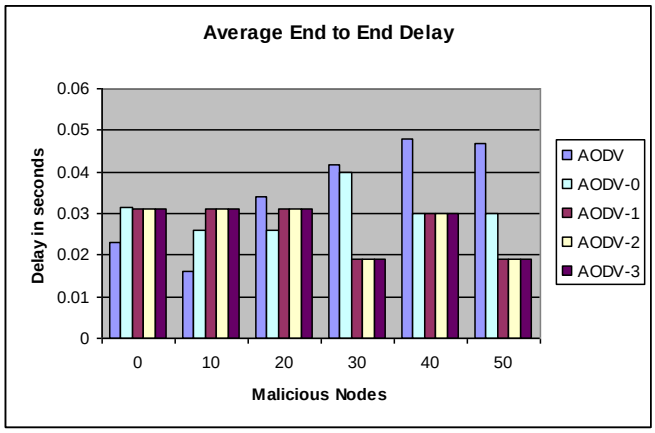

Figure 10(a). Average End to End delay for Malicious Nodes

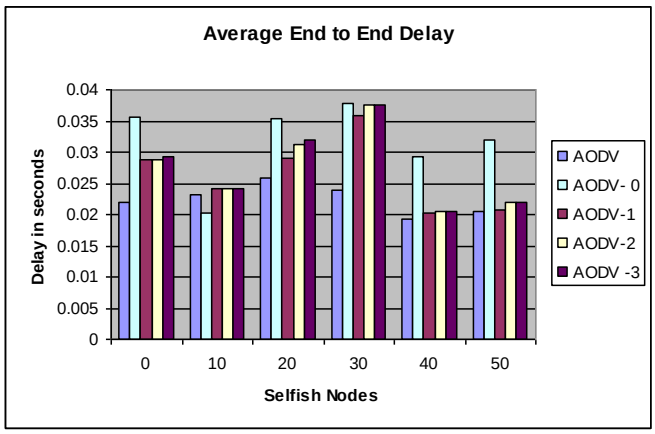

Figure 10(b). Average End to End delay for Selfish Nodes

4.6.5. Jitter: In a communication scenario stream line flow of data packets is necessary where in all the data packets follow their preceding packets with the same speed. In such a scenario the output will be smooth without any turbulence. If such a situation doesn't exist then the output is jerky and the jerks can be felt in the video and audio output. Flow of data packets will be streamline if each data packet takes equal time for traveling from source to destination. This quality of the communication scenario can be measured in terms of jitter [36-38] parameter. Figure 11(a) and Figure 11(b) show the jitter encountered by the data packets in different protocols.

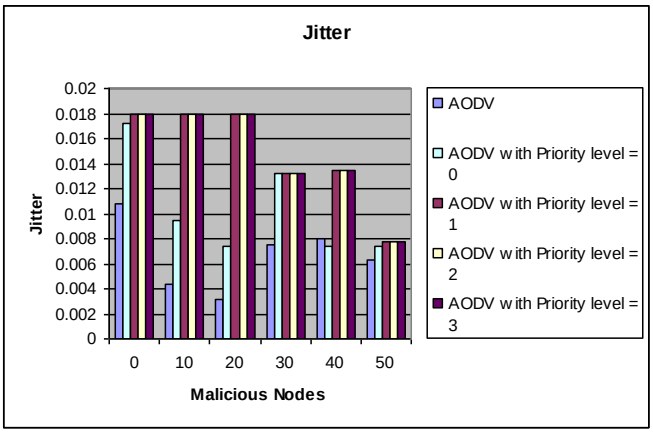

Figure 11(a). Average Jitter for Malicious Nodes

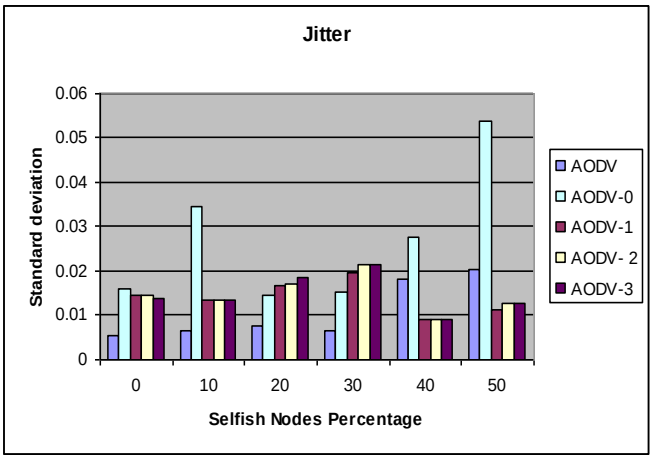

Figure 11(b). Average Jitter for Selfish Nodes

4.6.6. Packet Delivery Ratio

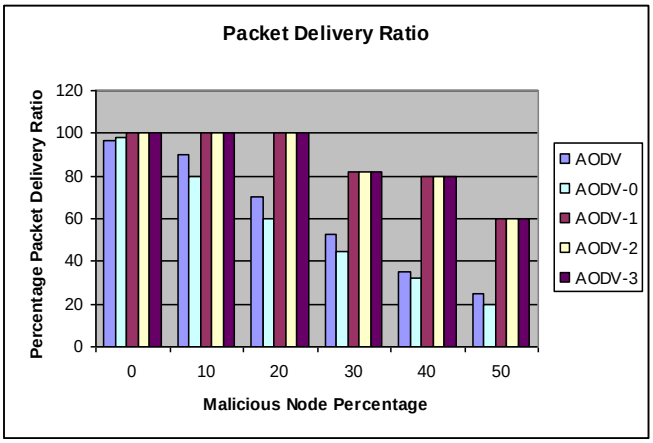

Figure 12(a). Average Packet Delivery Ratio for Malicious Nodes

It is the ratio of number of data packets successfully received at the destinations to the total number of data packets sent by various sources. At low concentration level of selfish and malicious nodes, the PDR of plain AODV is nearly same as that of AODV-1, 2, 3 but as the concentration of selfish and malicious nodes increases the PDR for plain AODV was found to be much lower in comparison to our protocol AODV-n as shown in Figure 12(a) and Figure 12(b). On analysis it was found that as the concentration of selfish and malicious nodes increases the nodes begin to drop data packets due to low battery power or due to their rogue behavior.

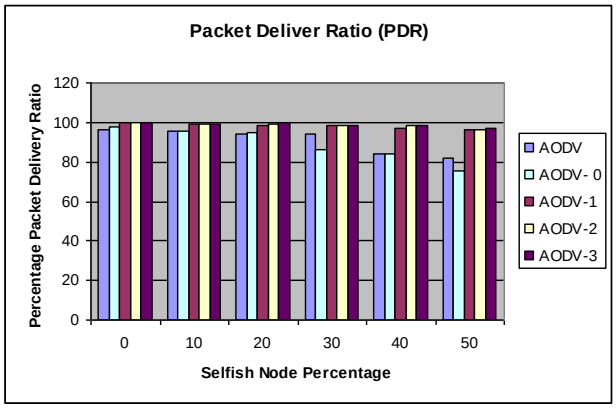

Figure 12(b). Average Packet Delivery Ratio for Selfish Nodes

4.6.7 Network Lifetime: The result shows the impact of selfish node concentration on network lifetime as the percentage of selfish nodes increases. Figure 13(a) shows the network lifetime on the basis of getting down of first node. Figure 13(b) show the network lifetime on the basis of getting of all nodes. Table 6 shows the simulation parameters used in the scenario.

Table 6. Simulation Parameters used in the Scenario

Default battery Power	2mah
Selfish node Battery Power	0.012mah
Energy model	Mica- Motes
Battery Depreciation Model	Linear

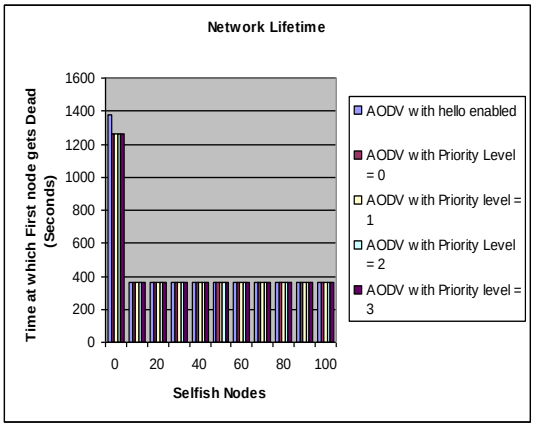

Figure 13(a). Network Lifetime for First Node

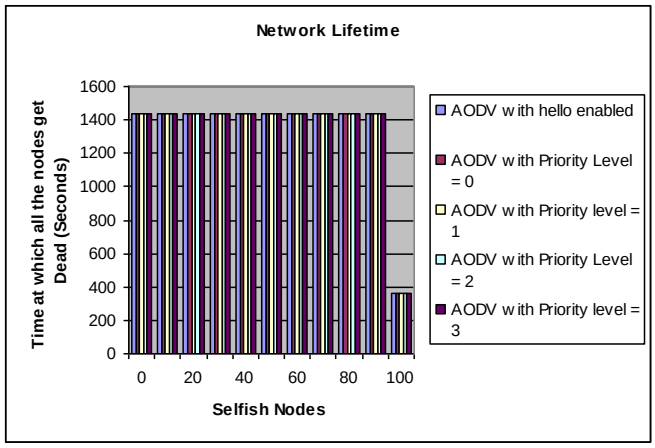

Figure 13(b). Network Lifetime for All Nodes

5. Analysis of Simulation Results

The analysis of simulation results indicate that in an environment devoid of malicious and selfish nodes plain AODV performs much better than AODV-n. As the concentration of malicious/ selfish nodes increases AODV-1, 2, 3 outperform the plain AODV. Many times, the performance of the AODV-1, 2, 3 protocols are better in an environment with large concentration of malicious/selfish nodes (40-50%) than the performance at the lower concentration of malicious/selfish nodes (10-30%). A careful scrutiny of the data showed that at high concentration of malicious/selfish nodes most of the routes formed were of the low hop count which allowed for easy passage of data packets leading to comparatively small amount of end to end delay and jitter. The performance of AODV-0 was the poor most where in the resources were used to collect data and compute the trust class but this information was not used to select the trust worthy intermediate nodes. Another note worthy feature of the simulation result was that there was not much difference between the performance of AODV-1, 2, 3 indicating that the choice of lower trust class works in the equally effective manner as in case of higher trust class. The network life time is very high when no node in the network is selfish but as the concentration of selfish nodes it decreases very fast as shown in Fig 13(a) and 13(b). On analysis it was observed that the energy dissipation in the nodes was mainly due to hello packets and not because of data packets sent from source to destination.

6. Conclusion

The analysis of the simulation results showed that if a feature like RECB is used to authenticate the node through response challenge mechanism then most of the trust worthy nodes can be easily identified. Also the low threshold of trust index as used in case of AODV-1 can provide a significant amount of requisite security. At very high concentration of malicious/selfish nodes most of the routes formed are of very low hop count and increasing the trust level threshold doesn't make the protocol much secure.

Acknowledgment

This work was supported by Eigen Technologies Private limited. The authors would like to thank Mr. Pranav and Mr. Ankur Tyagi for contributing Qualnet 5.0 code in support of the research.

References

[1] C. Mbarushimana and A. Shahrabi, "Comparative Study of Reactive and Proactive Routing Protocols Performance in Mobile Ad Hoc Networks", 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07), **(2007)**.
[2] E. Royer, C. K. Toh, "A review of current routing protocols for ad hoc mobile wireless networks", IEEE Personal Communications Magazine, vol. 6, no. 2, **(1999)**.
[3] Q. Lu, "A Survey on Vulnerability of Wireless Routing Protocols", Presentation, Virginia Polytechnic Institute and State University, **(2005)** July.
[4] P. Argyroudis, "Current state of secure routing for mobile ad hoc networks", Trinity College Dublin Security Interest Group, **(2002)** November.
[5] Wikipedia, The Free Encyclopaedia, **(2005)** July.
[6] B. S. Manoj and C. S. R. Murthy, "Transport Layer and Security Protocols for Ad Hoc Wireless Networks", Prentice Hall PTR, **(2005)** January.
[7] S. Buchegger and J. -Y. Le Boudec, "Self-Policing Mobile Ad Hoc Networks by Reputation Systems", Advances in Self-Organizing Networks, IEEE Communications Magazine, **(2005)** July.
[8] L. Blazevic, L. Buttyan, S. Capkun, S. Giordano, J. P. Hubaux and J. Y. Le Boudec, "Self- Organization in Mobile Ad-Hoc Networks: the Approach of Terminodes", IEEE Communications Magazine, vol. 39, no. 6, **(2001)** June.
[9] S. Marti, T. J. Giuli, K. Lai and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", Proc. of MobiCom 2000, Boston, **(2000)** August.
[10] L. Buttyán and J. -P. Hubaux, "Nuglets: a Virtual Currency to Stimulate Cooperation in Self- Organized Mobile Ad Hoc Networks", Technical report No. DSC/2001/001, Swiss Federal Institution of Technology, Lausanne, **(2001)** January, http://icawww.epfl.ch/hubaux/.
[11] S. Gupta, C. K. Nagpal and C. Singla,"Impact of Selfish Node Concentration in MANETs", International Journal of Wireless & Mobile Networks (IJWMN), vol. 3, no. 2, **(2011)** April.
[12] L. Buttyán and J. -P. Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks", ACM/Kluwer Mobile Networks and Applications, vol. 8, no. 5, **(2003)** October.
[13] S. Zhong, J. Chen and R. Yang, "Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks", In Proceedings of IEEE Infocom '03, San Francisco, CA, **(2003)** April.
[14] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks", In Mobile Computing and Networking, **(2000)**, pp. 275–283, http: //citeseer.nj.nec.com/zhang00intrusion.html.
[15] Y. Zhang, W. Lee and Y. -A. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks", to appear in ACM Wireless Networks (WINET), vol. 9, **(2003)**, http://www.wins.hrl.com/people/ygz/papers/ winet03. pdf.
[16] M. N. Lima, H. W. da Silva, A. L. dos Santos and G. Pujolle, "Requirements for survivable routing in MANETs", In International Symposium on Wireless Pervasive Computing IEEE 2008, (Reference gives disadvantage of cryptography, Need for Security mechanisms), **(2008)**.
[17] K. Balakrishnan, J. Deng and V. K. Varshney, "TWOACK: Preventing Selfishness in Mobile Ad Hoc Netwotks", In Proc. of WCNC, **(2005)**.
[18] P. Dewan, P. Dasgupta and A. Bhattacharya, "On Using Reputations in Ad Hoc Networks To Counter Malicious Nodes", In Proc. of ICPADS, **(2004)**.
[19] S. Bansal and M. Baker, "Observation-based Cooperation Enforcement in Ad Hoc Networks", Arxiv preprint cs/0307012, **(2003)**.
[20] K. Liu, J. Deng, P. K. Varshney and K. Balakrishnan, "An Acknowledgment-Based Approach for The Detection of Routing Misbehavior in MANETs", IEEE TMC, **(2007)**.
[21] P. Michiardi and R. Molva, "CORE: A Collaborative Reputation Mechanism To Enforce Node Cooperation in Mobile Ad Hoc Networks", In Proc. of CMS, **(2002)**.
[22] S. Buchegger and J. -Y. L. Boudec, "Performance Analysis of the Confidant Protocol", In Proc. of MOBIHOC, **(2003)**.
[23] S. Marti, T. J. Giuli, K. Lai and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", In Proc. of MOBICOM, **(2000)**.
[24] Q. He, D. Wu and P. Khosla, "SORI: A Secure and Objective Reputation-based Incentive Scheme for Ad-hoc Networks", In Proc. of WCNC, **(2004)**.
[25] S. Buchegger and J. Y. Leboudec, "The Effect of Rumor Spreading in Reputation Systems for Mobile Ad Hoc Networks", In Proc. of WIOPT, **(2003)**.
[26] B. Zong, F. Xu, J. Jiao and J. Lv, "A Broker-Assisting Trust and Reputation System Based on Artificial Neural Network", In Proc. of SMC, **(2009)**.
[27] M. T. Refaei, L. A. DaSilva, M. Eltoweissy and T. Nadeem, "Adaptation of Reputation anagement Sytems to Dynamic Network Conditions in Ad Hoc Networks", IEEE TOC, **(2010)**.

[28] S. Buchegger and J. Y. Le Boudec, "A Robust Reputation System for Mobile Ad-hoc Networks", In Proc. of P2PEcon, **(2004)**.
[29] A. A. Pirzada, C. McDonald and A. Datta, "Performance comparison of trust-based reactive routing protocols", IEEE Trans. on Mobile Computing, vol. 5, no. 6, **(2006)**, pp. 695-710.
[30] A. A. Pirzada and C. McDonald, "Establishing Trust in Pure Ad Hoc Networks", Proc. 27th Australasian Computer Science Conf.(ACSC), vol. 26, **(2004)**, pp. 47-54.
[31] A. A. Pirzada and C. McDonald, "Kerberos Assisted Authentication in Mobile Ad Hoc Networks", Proc. 27th Australasian Computer Science Conf. (ACSC), vol. 26, **(2004)**, pp. 41-46.
[32] L. Blazevic, L. Buttyan, S. Capkun, S. Giordano, J. P. Hubaux and J. Y. Le Boudec, "Self-Organization in Mobile Ad-Hoc Networks: the Approach of Terminodes", IEEE Communications Magazine, vol. 39, no. 6, **(2001)** June.
[33] L. Abusalah, A. Khokhar and M. Guizani, "TARP: Trust-Aware Routing Protocol", Proc. ACM Int'l. Wireless Communication and Mobile Computing Proceeding-IWCMC, Vancouver, Canada, **(2006)** August.
[34] S. Gupta and C. Kumar, "Shared Information for Mobile Ad hoc Networks", IJWMN, vol. 2, no. 1, (2010) February.
[35] X. Zhao, Z. You, Z. Zhao, D. Chen and F. Peng, "Availability Based Trust Model of Clusters for MANET", in 7th International Conference on Service Systems and Service Management ICSSSM, **(2010)**.
[36] H. Dai, Z. Jia and Z. Qin, "Trust Evaluation and Dynamic Routing Decision Based on Fuzzy Theory for MANETs", Journal of Software, vol. 4, no. 10, **(2009)** December, pp. 1091-1101.
[37] M. Jakobsson, J. Hubaux and L. Buttyan, "A Micropayment Scheme Encouraging Collaboration in multi-hop Cellular Networks", In Proc. of Financial Cryptograph, **(2003)**.
[38] L. Buttyan and J. Hubaux, "Enforcing Service Availability in Mobile Ad-Hoc WANS", In Proc. of MOBIHOC, **(2000)**.
[39] J. Crocraft, R. Gibbens, F. Kelly and S. Ostring, "Modeling Incentives for Collaboration In Mobile Ad Hoc Networks", Performance Evaluation, **(2004)**.
[40] L. Anderegg and S. Eidenbenz, "Ad Hoc-VCG: A Truthful And Cost- Efficient Routing Protocol for Mobile Ad Hoc Networks With Selfish Agents", In Proc. of MOBICOM, **(2003)**.
[41] H. Janzadeh, K. Fayazbakhsh, M. Dehghan and M. S. Fallah, "A Secure Credit-Based Cooperation Stimulating Mechanism for MANETs Using Hash Chains", In Elservier, FGCS, **(2009)**.
[42] Z. Li and H. Shen, "Game-Theoretic Analysis of Cooperation Incentive Strategies in Mobile Ad Hoc Networks", accepted for publication in future issues of IEEE Transactions on Mobile Computing.
[43] M. Hassan and R. Jain, "High Performance TCP/IP Networking: Concepts, Issues, and Solutions", Upper Saddle River, NJ: Pearson Prentice Hall, **(2004)**.
[44] "Monitoring Your IP Telephony Network.", white paper, NEC Unified Solutions, **(2004)**.
[45] L. Qi and C. Di, "Analysis and Improvement of TFRC Congestion Control Mechanism", in Proc. Wireless Communications, Networking and Mobile Computing, **(2005)**, pp. 1149-1153.