International Journal of Networks and Communications 2020, 10(1): 10-19
DOI: 10.5923/j.ijnc.20201001.02

Optimized Trust-Based DSR Protocol to Curb Cooperative Blackhole Attacks in MANETs Using NS-3

Ephantus Gichuki Mwangi*, Geoffrey Muchiri Muketha, Gabriel Ndung'u Kamau

School of Computing and Information Technology, Murang'a University of Technology, Murang'a, Murang'a, Kenya

Abstract MANETs Communication relies on special routing protocols that make security a challenging endeavor. MANETs are open to a range of active and passive attacks; black hole attack is an active attack affects the network layer. Cooperative black hole attack is a form of denial of service attack comprised of more than one black hole nodes that collaborate in order to drop data packets during communication process. In our study, we used the concept of trust to extend the DSR protocol in order to mitigate cooperative black hole attacks that leads to loss of data packets. The paper proposes an Optimized Trust-Based Dynamic Source Routing protocol. The proposed protocol integrates dynamic trust and friendship functions in the standard DSR protocol. The proposed protocol was designed, implemented and simulated in Network Simulator version 3 (NS-3). Simulation results indicate that the proposed protocol is superior to standard Dynamic Source Routing (DSR) protocol and Ad hoc On Demand Vector (AODV) protocols used as the benchmark protocols; in terms of packet delivery ratio, routing overhead and end-to-end delays and throughput used as performance metrics. The Optimized Trust-Based DSR protocol had a packet delivery ratio of above 95%, routing overhead of about 4.75% and an end-to-end delay of between 0.9 seconds and 1.65 seconds and a throughput of 95.6 Kbps.

Keywords Routing protocol, Trust-Based Routing, OTB-DSR Protocol, Cooperative Blackhole and Composite Trust Values

1. Introduction

The advent of mobile devices brought a paradigm shift in network communication. Mobile technology has led to the emergence of Mobile ad hoc networks (MANETs). MANETs are special types of wireless networks comprised of mobile nodes [1]. The network is infrastructureless and has no centralized management. Nodes in MANETs freely join and leave the network at their own will, hence making the network topology highly dynamic. The nodes cooperate in forwarding data packets from source to destination using special routing protocols. The protocols used in wired networks are not applicable to wireless networks [2]. Each node in a MANET has a transceiver gadget which makes it to acts as both a router and a host. A node intending to communicate with other nodes in MANET establishes a route using the special routing protocols [1].

Several routing protocols have been designed to optimize MANETs routing security [2], [6]. The design of secure routing protocols has been surrounded by design issues such as dynamic network topology, constrained bandwidth, limited battery power, error prone wireless channel, and unpredictable node mobility. The unique features of MANETs make most of the security solutions designed for wired networks inappropriate for mobile ad hoc networks. Further, the dynamic nature of MANETs makes it difficult to develop secure ad hoc routing protocols [3].

The aim of our study was to develop an Optimized Trust-Based DSR protocols by extending the standard DSR protocol using dynamic trust and friendship functions. The purpose of dynamic trust function was to calculate trust values for the individual nodes in MANETs based on how successful or unsuccessful they forward data packets to their immediate neighbours. Further, friendship function was used to classify nodes in various levels of friendship based on composite trust values (CTVs) generated from the dynamic trust function.

MANETs routing protocols are categorized as: reactive routing protocols (on demand), proactive routing protocols (table driven) and hybrid protocols. In reactive routing protocols routes are created on-demand whenever a source node intends to send data packets to a destination node. This means that only nodes which participate in active routes maintain the routing information. Ad hoc On-demand Distance Vector (AODV), Dynamic Source Routing (DSR)

* Corresponding author:
egmkuc@gmail.com (Ephantus Gichuki Mwangi)
Published online at http://journal.sapub.org/ijnc
Copyright © 2020 The Author(s). Published by Scientific & Academic Publishing
This work is licensed under the Creative Commons Attribution International License (CC BY). http://creativecommons.org/licenses/by/4.0/

and Link Aware Routing (LAR) are some of the examples of reactive routing protocols [6]. In proactive protocols, each node maintains complete routing information of the network in a routing table. Change in the network topology due to nodes mobility leads to automatic updating of routing tables in all the nodes. Examples of proactive routing protocols are Destination Sequenced Distance Vector (DSDV), Global State Routing (GSR) and HSR. Hybrid protocols are as a result of blended features of both proactive and reactive routing protocols [4].

MANETs Routing protocols govern how data packets flow from source to destination nodes [1]. The uniqueness of MANETs has exposed these protocols to a variety of attacks. The attacks can either be from within or outside the network. Studies conducted in this domain indicate that there is need to enhance existing MANETs routing protocols so that they can effectively mitigate network attacks as they transmit data with higher efficiency [6]. DSR is a reactive routing (on-demand) protocol that relies on the concept of source routes in order to transmit data packets. It uses two primary mechanisms; route discovery and route maintenance.

When a source node wants to transmit some data packets, it initiates a route discovery mechanism by first searching for a source route from the routes saved in its routes' cache. The source routes are maintained by every node in the network. If no source route is found in the sending node's cache, it initializes route request process by sending a RREQ packet to its immediate neighbours. The nodes using DSR protocol carries complete routing information from source to destination node in its packet header. However, the routes in the cache may be stale or broken. The DSR protocol uses route maintenance mechanism to validate all its source routes. The mechanism is managed using route error messages or acknowledgements. Previous studies show that the DSR protocol suffers some transmission inefficiencies attributed to broken links, invalid routes and inability to effectively identify malevolent nodes in the network during source routes establishment [6].

The concept of trust among nodes in MANETs can be used to identify and eliminate malicious nodes in a network [7], [8]. Further, trust can be used to determine the degree of reliance among interacting nodes. Additionally, trust can be used to determine which entities belong to which circle of friendship. Trust is dynamic; a member of a certain circle of friendship can be promoted to a higher circle or demoted to a lower one depending on the variance of trust. Furthermore, every circle of friendship can be assigned a level of trust.

The rest of the paper is organized as follows; section one introduces the paper, section 2 discusses the related works, while section 3 presents a trust model, section 4 presents trust based routing, section 5 presents protocol's algorithms, section 6 describes simulation environment, section 7 presents results and discussion, and section 8 presents conclusions and future work.

2. Related Work

El-Haleem and Ali [10] proposed a two node-disjoint routes protocol for Isolating Dropper (TRIDNT) in MANETs. TRIDNT permits some degree of selfishness to a selfish node. This gives it a chance to declare itself to its neighbors as selfish, hence reducing the misbehaving nodes searching time. When a malicious behaviour is detected within the paths, then the path searching tool automatically starts to detect and isolates them. TRIDNT protocol was not simulated; its performance analysis relied on mathematical model which is not sufficient to validate this protocol.

In [11], Airehrour, Gutierrez and Ray proposed GradeTrust, a Secure Trust Based Routing protocol for MANETs. GradeTrust is based on trust levels of network nodes. In this protocol, all nodes are categorized into three sets namely: trusted friends (TF), friends (F) and possible friends (PF). During the routing process GradeTrust uses the three trust metrics to compute secure routes. These trust metrics help in isolating routes with black hole nodes. In terms of performance metrics, that is packet delivery ratio, end to end delay and trust compromise; GradeTrust protocol performed much better than AODV and DSR used as the benchmark schemes. However, on average the packet delivery ratio of GradeTrust was below 80% and decreased with increase in speed of node mobility. Further, trust compromise increased with increase in the number of nodes in the presence of black hole nodes.

Sultana and Ahmed [12] implemented a secure AOMDV protocol using Elliptic Curve Cryptography (ECC) to prevent loss of data packets from malicious attacks in the network. AOMDV a reactive routing protocol is an extension of AODV routing protocol. ECC is an encryption technique which provides security with smaller key size compared to other public key encryption. Simulation experiment was configured in three different kinds of environments: secure environment without malicious nodes, hostile environment with black hole attacks and an environment with ECC implementation by the agent. Simulation results showed that AOMDV is more superior to standard AODV protocol, although not completely restraint from all types of attacks. The study did not indicate whether AOMDV protocol is sufficient enough to mitigate collaborative attacks.

In [13] Sreenath at al. proposed an algorithm using Secure Enhanced-On Demand Multicast Routing Protocol (EODMRP). The algorithm focused on improving the security of MANETs against multicast attacks. The proposed algorithm was implemented and tested using GloMoSim (2.03). Further, after simulation, performance analysis showed improvement in packet delivery ratio in presence of black hole attack, with marginal rise in average end to end delay and normalized routing overhead. Additionally, simulation showed that this technique worked well for flooding attacks even when the identity of the malicious nodes was unknown. This mechanism did not use any additional network bandwidth during data transmission. However, the mechanism was only intended for multicast routing protocols. There is a need to extend this study by developing a solution for proactive protocols through the change of implementation techniques.

Jhaveri [14] proposed a modified RAODV (MR-AODV) protocol, an enhancement of R-AODV protocol. This protocol was subjected to varying network size, mobility, traffic load and malicious attacks through a simulation process. Simulation results showed that MR-AODV isolates black hole nodes during route discovery phase just as R-AODV and sets up a secure route for data transmission. The study showed that MR-AODV protocol was superior to R-AODV protocol used as benchmark; hence a better solution for MANETs against black hole attacks. However, MR-AODV protocol needs further enhancement to improve network efficiency in terms of packet delivery ratio as the number of malicious nodes increases. Further, the MR-AODV protocol needs to be enhanced in order to mitigate cooperative black hole attacks.

Gupta and Woungang [15] proposed a trust-based security protocol (TSP) against PRoPHET (PBH scheme) routing protocol for opportunistic networks (Oppnets). The aim of the study was to compare the effectiveness of the two protocols. Simulation results showed that the PBH scheme led to higher wastage of network resources while the TSP contributed in reduction of network bandwidth usage by avoiding the additional message replicas that would have been transmitted to the black hole nodes. These findings indicated that TSP is a better routing protocol to curb black hole attacks than PBH scheme. However, TSP needs to be enhanced in order to provide the following functions: calculation of the SGV values in case of randomized behavior of malicious nodes, calculation of credits for evaluation of the trust values of nodes and capturing node's relative delivery probability for higher trusted. Further, TSP needs to be enhanced to be able to detect and prevent cooperative black hole attacks.

In [16], Arya et al. recommended a trusted AODV routing algorithm for detecting and mitigating collaborative black hole attacks in MANET. Simulation experiment indicated that in the presence of collaborative black hole attack AODV protocol used more energy than trusted AODV algorithm. Further, it was noted that throughput and packet delivery ratio of trusted AODV algorithm was better compared to AODV protocol. This was an indication that trusted AODV routing algorithm is a superior compared to AODV protocol and can do better in protecting MANETs against collaborative black hole attacks.

Woungang et al. [17] introduced DBA-DSR a novel scheme for detecting blackhole attacks in MANETs. Simulation results showed that the proposed scheme performed better than DSR scheme in terms of network throughput and packet delivery ratio. However, this scheme needs to be extended in order to detect and prevent cooperative blackhole attacks in MANETs. Further, the throughput of proposed scheme needs to be enhanced as it was below 80%; while its end to end delay needs to be maintained to acceptable levels.

The reviewed literature indicates some underlying gaps in existing protocols that led to the development of the proposed OTB-DSR protocol. The gaps are as follows; 1) most of the existing protocols do not have the capacity to mitigate cooperative blackhole attacks with a higher efficiency. This leads to compromised data transmission in MANETs. 2) Most of the existing protocols have not embraced the concept of trust based routing which can help in mitigating collaborative attacks.

3. The Proposed Trust Based Routing Management Model

Trust based routing is a technique where nodes establish routes based on the level of trust amongst other nodes in a network. In this technique past experience, interactions and recommendations from other nodes forms the basis of trust. The technique establishes a mechanism of awarding trust values to a node which are finally used to promote it to different levels of trust based on aggregate successive transmissions. The trust values and trust levels help the source node to identify the most trusted nodes during route discovery. Nodes that successfully route data packets amongst their peers are considered more trusted than others and are awarded higher trust levels [20]. The study adopted the concept of Trust Based Routing in extending DSR protocol. The formula 1 below is a derivation of a trust management model based on human interaction concept. According to the formula, human trust is a fraction derived from the difference between successful and failed interactions attempts between any two persons divided by summation of successful and failed interactions attempts; multiplied by a time growth factor (TGF). The TGF is a variable that represents the growth or decay of trust with time.

$$\mathrm{HT} = \frac{\text{Time Growth Function}^{-\alpha t} * (\text{Successful Interaction} - \text{Failed Interactions})}{(\text{Successful Interactions} + \text{Failed interaction})} \tag{1}$$

Mathematically, formula 1 can be represented as indicated in equation 2.

$$HT^{x,y} = \frac{\mathrm{TGF}^{-(\mathrm{x,y})\alpha\mathrm{t}}\,(SI^{x,y} - \mathrm{FI}^{x,y})}{(SI^{x,y} + \mathrm{FI}^{x,y})} \tag{2}$$

Where $HT^{x,y}$ is the trust between any two interacting parties. The variable $\mathrm{TGF}^{(\mathrm{x,y})-\alpha\mathrm{t}}$ is a factor of growth or decay of trust over time. The expression $(SI^{x,y} - \mathrm{FI}^{x,y})$ represents the difference between successful and failed interaction attempts between any two interacting parties. Further, expression $(SI^{x,y} + \mathrm{FI}^{x,y})$ represents the summation of both successful and failed attempts between any two parties.

In networking environs, the interactions of nodes can be equated to the behaviour of human beings in social networks as indicated in formula 2. Further, trust among nodes in a

MANET can be quantified through a model. In our study, we derived a trust management model based on how nodes build trust based on the interactions amongst themselves overtime. The basis of this trust is anchored on both positive and negative interactions among interacting the nodes. To demonstrate how this trust relationship can be modeled and quantified among neighbouring nodes in a MANET, equation 3 was adopted as the basis of our model.

$$NTV^{x,y} = \sum_{i=1}^{n}\left(\frac{e^{-(\mathrm{x,y})\alpha} *(NSI^{x,y} - \mathrm{NFI}^{x,y})}{(NSI^{x,y} + \mathrm{NFI}^{x,y})}\right)/n \qquad (3)$$

Where $NTV^{x,y}$ is the composite node's trust value, $e^{-(\mathrm{x,y})\alpha}$ is an expression that shows the growth on nodes trust with time. Further, expression $(NSI^{x,y} - \mathrm{NFI}^{x,y})$ shows the difference between successful and failed interactions attempts between two nodes. Additionally, expression $(NSI^{x,y} + \mathrm{NFI}^{x,y})$ is the summation of both successful and failed interactions. Finally, n is an integer value that represents the total number of nodes that recommend trust to a certain node.

4. Design of the Proposed OTB-DSR Protocol

This study has extended standard DSR protocol using Dynamic Trust and Friendship functions which were informed based on the concept of trust values and levels discussed above. The two parameters formed the basis of classification of nodes in our proposed OTB-DSR protocol.

4.1. Architecture of OTB-DSR Protocol

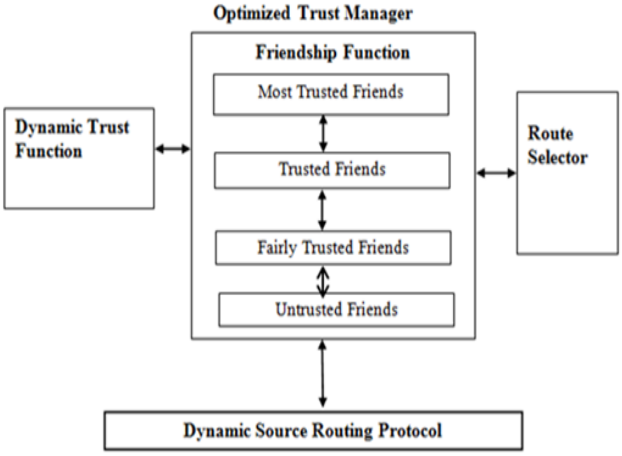

Figure 1. OTB-DSR Protocol Architecture

The proposed protocol is made up of two key segments: Optimized Trust Manager and the Standard DSR protocol. Figure 1 shows the interrelationship of the various components in the architecture of the proposed Optimized Trust-Based DSR protocol. The DSR protocol forms the core segment and directly interacts with the Optimized Trust Manager. The Optimized Trust Manager is made up of three components: Dynamic Trust Function, Friendship Function and Route Selector. The three components are interrelated and directly interact with each other during route discovery in order to establish the optimal route from the node's cache.

4.2. Design of the Dynamic Trust Function

The purpose of this function is to calculate Composite Trust Values (CTV) of every node in the network using a trust model. The principle behind Composite Trust Value calculation is earning or losing points bases on successful/unsuccessful packet transmissions to its immediate neighbours. In this technique, the next hope neighbours of every node has the responsibility of continuously recommending Trust Values (TVs) by sending acknowledgement packets (ACK) when they receive data packets successfully. A node which successfully transmits a packet to its next hop neighbour is appraised by one point which is automatically incremented in CTV and stored in the Trust Wallet (TW) of a node.

In case a node fails to forward a data packet to its immediate neighbour either due to selfishness or malicious intentions, a negative acknowledgement (NACK) is sent. A NACK makes a node lose a point which is automatically decremented from CTV of a node. Nodes joining the network for the first time are automatically assigned CTV of zero (0) points. The TVs from all immediate neighbouring nodes are then forwarded to the node's routing table in order to compute CTV; which is finally stored in the TW.

Equation 4 shows how CTV are computed for an individual node in a given route.

$$CTV^{x,y} = \sum_{i=1}^{n}(K\,\mathrm{e}^{-(1-\mathrm{k})})/n \qquad (4)$$

Where: CTV represents composite trust values awarded to a node as a result of successive transmissions, e represents the exponential function, K represents a ratio; that is $\frac{(\mathrm{NSI}^{x,y} - \mathrm{NFI}^{x,y})}{(\mathrm{NSI}^{x,y} + \mathrm{NFI}^{x,y})}$, i represent the number of neighbouring nodes recommending Trust Values and n represents the total nodes that participated in trust recommendation (whether positive or negative recommendation).

The CTVs for nodes in a certain route are used to calculate Route Trust Value (RTV) for that route. Equation 5 shows how Route Trust Value (RTV) for a given route is computed.

$$RTV = \left(\sum_{i=1}^{n} CTV_i\right)/n \qquad (5)$$

Where: i represent individual node; n represent total nodes in a given route.

If in a node's cache there is more than one source route, the route with the highest RTV is selected for packet transmission. Further, if there is more than one route with the same RTV, the route with the least hop count (shortest route to destination) is selected packet routing. Optimized Trust-Based Dynamic Source routing protocol requires two extra fields in its node's routing table in order to accommodate the routing technique. The two fields are: Composite Trust Value (CTV) and Friendship Level (FL) fields. The purpose of FL field is to store the friendship level a node has been accorded by its neighbouring nodes based on how successful or unsuccessful it has participated in packet transmissions. The flowchart indicated in figure 2 shows how OTB-DSR protocol calculates and updates CTVs and RTVs in a MANET.

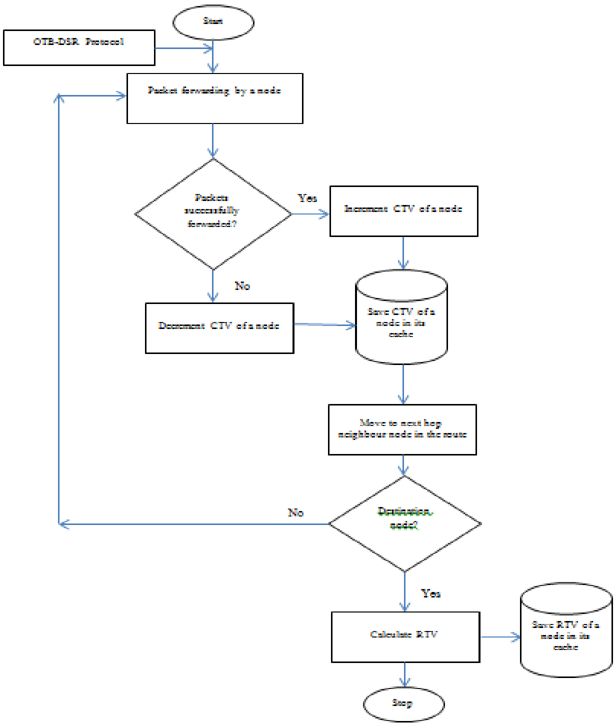
Start
OTB-DSR Protocol
Packet forwarding by a node
Packets successfully forwarded?
Yes
Increment CTV of a node
No
Decrement CTV of a node
Save CTV of a node in its cache
Move to next hop neighbour node in the route
No
Destination node?
Yes
Calculate RTV
Save RTV of a node in its cache
Stop

Figure 2. Operation flowchart of the OTB-DSR Protocol

4.3. Design of the Friendship Function

This function uses threshold trust values to classify nodes into social friendship groups based on successful interaction experiences during data packet transmission. A node can be classified in any of the four friendship levels: Untrusted Friends, Fairly Trusted Friends, Trusted Friends and Most Trusted Friends. A node that joins the network for the first time is automatically assigned a Trust Value (TV) of zero points. Nodes cumulatively build their TVs based on successfully packet transmission to their immediate neighbours. Any node with TVs less than four points is marked as malicious node. The malicious nodes are not considered during routes formation unless they are the only existing nodes along that route. Nodes under Untrusted Friends level are the nodes that have met trust threshold value of four points by successfully forwarding data packets to their immediate neighbours' atleast four times consecutively since they joined the network.

A node under Fairly Trusted Friends level must first meet the trust threshold value of four points in order to be allowed to participate in data packet transmission. Further, the node must have successfully passed data packets to its one hop neighbours atleast two times consecutively since it was enrolled under Untrusted Friends level. Routes with nodes under this level have the least chances of being selected to participate in any packets transmission responsibility.

Nodes that are promoted to Trusted Friends level are the nodes that have successfully passed data packets atleast more than two times since they joined Fairly Trusted Friends level. Route with nodes under this category have fair chances of being selected to participate in packet transmission. The Most Trusted Friends level belongs to nodes that have successfully passed data packets to their one hop neighbours atleast two times consecutively since they joined the Trusted Friends level and have never dropped any data packets since they joined the network. A source route with most of these nodes in the route cache has the highest chance of being selected for participation in packet routing. The equations 6 to 9 shows how nodes trust levels are classified into social friendship groups based on the successful interactions with immediate neighbours during data packet transmission.

$$FL_{uf} = (M * k) \tag{6}$$

$$FL_{ftf} = (M * k) + (2 * k) \tag{7}$$

$$FL_{tf} = (M * k) + (4 * k) \tag{8}$$

$$FL_{mtf} = (M * k) + (6 * k) \tag{9}$$

Where M is the threshold trust value of a node; M = 4 points, K is trust constant; K = 0.1, FL denotes friendship level. CTV>M, (M*K) < FL<=1.

Table 1 show the trust value limits applied in our proposed OTB-DSR protocol based on the above equations. Xn represents any node in the MANET.

Table 1. Social Group Trust Value Limits

S.No	Node	Trust Value Limit	Social Group/Level
	Xn	FLuf<0.4	Untrusted Friends
	Xn	0.4=< FLftf<=0.6	Fairly Trusted Friends
	Xn	0.6=< FLtf<=0.8	Trusted Friends
	Xn	0.8=< FLmtf<=1	Most Trusted Friends

5. Algorithm

This is a logical flow of steps that define a solution to an underlying problem. The study designed two algorithms for the dynamic trust and friendship functions. These algorithms give a detailed procedure of how the two functions were integrated in the DSR protocol.

5.1. Algorithm of Dynamic Trust Function

The dynamic trust function algorithm awards individual nodes in a MANET trust points based on how successful or unsuccessful they interact with their neigbours. A node that successful passes a data packet to its neighbour is awarded trust value of one point. Further, any node that does not pass a data packet to its neigbour either due to selfish or malicious intentions is denied trust value of one point. The trust values are saved in Composite Trust Value field of a node's data structure. The value in this field is updated every time a node participates in a data transmission process. The algorithm of Dynamic Trust Function is represented in figure 3. The algorithm is a sub module of the OTB-DSR protocol.

```
Algorithm DynamicTrust_Function
{[Start]
Declare CTV, TVs, TW, srcAddress, interAddress, dstAddress;
Initialize CTV to Zero
Initialize Source_IPAddress and Destination_IPAddress
do {
            If Reply (RREP) from Real Destination node is Genuine{
             Increment Intermediate Node's Cumulative Trust Value by
          one
            else
            decrement Intermediate Node's Cumulative Trust Value by
one}
            Assign Composite Trust Values of Intermediate node to its
Trust           Wallet
            Increment Intermediate Node's IPAddress by one
            dstAddress=interAddress
While (dstAddress != Destination_IPAddress)
[End]}
```

Figure 3. Dynamic Trust Function Algorithm

5.2. Algorithm of Friendship Function

```
Algorithm Friendship_Function
{[Start]
Declare Variables Friendshiplevel, UT_Count, F_Count, TF_Count,
MTF_Count, TrustThresholdValue (boolean);
  If Node's CTV > 4points {
      TrustThresholdValue set to true
      FriendshipLevel equals "UnTrustedFriends";
     Elseif TrustThresholdValue=true and Node CTVs greater or equal
to       6 points{
         FriendshipLevel equals "FairlyTrustedFriends";
         F_Count incremented by 1;}
      Elseif (FriendshipLevel equals "FairlyTrustedFriends"and Node
        CTVs greater or equal to 8){
          FriendshipLevel equals "TrustedFriends";
          TF_Count incremented by 1;}
     Elseif (FriendshipLevel equals "TrustedFriends"and Node's CTVs
        greater or equal to 10) {
          FriendshipLevel equals "MostTrustedFriends";
          MTF_Count incremented by 1;}
         Display FriendshipLevel of a Node;
[End]}
```

Figure 4. Friendship Function Algorithm

The friendship function is a sub module of the OTB-DSR protocol. The purpose of this algorithm is to classify nodes in different levels of trust based on composite trust values (CTV) awarded by their neighbours. In this algorithm, there are four levels of friendship; untrusted friends, fairly trusted friends, trusted friends and most trusted friends. Nodes whose CTV points fall between 4 and 5 since they joined MANET are classified as '*UntrustedFriend*'. Additionally, nodes whose CTV points fall between 6 and 7 since their promotion to the previous friendship level are classified as '*FairlyTrustedFriends*'. Further, nodes whose CTV points fall between 8 and 9 since their promotion to the previous friendship level are classified as '*TrustedFriends*'. Finally, nodes whose CTV points are greater than 10 since their promotion to the previous friendship level are classified as 'Most*TrustedFriends*'. Figure 4 shows the implementation of friendship function algorithm.

6. Simulation Environment

The platform for simulation of OTB-DSR protocol was Ubuntu linux Operating System version 18.03. Ubuntu Operating System is open source; which means it can be freely downloaded from the Internet. Recent upgrades of the Ubuntu operating system are also found inform of patches downloadable from the Internet. The minimum hardware requirements for Ubuntu Operating system are; core 2 Duo processor or higher, memory of 2 GHz or higher and hard disk capacity of 500 GB or higher. Ubuntu operating system is compatible with NS-3 simulator.

In our simulation experiment, two assumptions were made, that is; data packets can only be lost as a result of them being dropped by malicious nodes and nodes that participate in packet transmission have enough battery power to sustain the transmission process.

a) NS-3 Simulator

NS-3 is a discrete-event network simulation tool developed by Tom Henderson, et al. [18], [19] in the year 2006 for Internet systems and was mainly targeted for educational use and research purposes. NS-3 was built as a replacement for NS-2. The new simulator completely abandons backward-compatibility with NS-2. NS-3 is written from scratch, using C++ programming language and Python with scripting capability. The simulator has a set of network simulation models implemented as C++ objects and wrapped in Python [18]. In NS-3 users write Python or C++ application that starts a set of simulation models that defines their simulation scenario. Building and compilation of NS-3 applications is done in Python [19].

NS-3 software mainly target the system needs by first building the libraries of software development environment, and then build the user application program. The Network Simulator tool is built on the concepts of independent tracing of sources and sinks, and a uniform mechanism for connecting sources to sinks [18], [19]. NS-3 design simulations are built using Use Case models to allow the simulator to interact with real world. Figure 5 show the internal architecture of NS-3 simulator.

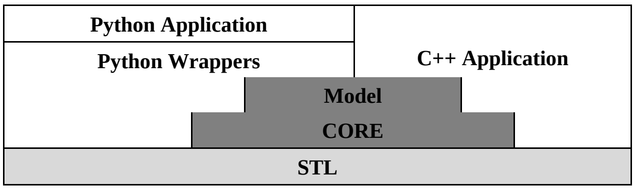

Figure 5. NS-3 Architecture

b) Simulation Parameters

Simulation area was set in a rectangular pane measuring 1500×1000m. Fifty genuine mobile nodes were installed. Further, two to ten black hole nodes were installed in our three simulation scenarios respectively. Simple attack model was set to enable the blackhole nodes to initiate the attacks. The channel of communication among nodes was set to User Datagram Protocol (UDP). In order for the nodes to maneuver within the simulation area, propagation model was set to Radom Way Point (RWP) model. The connection between nodes was set using the NS-3 WI-FI model. The nodes were configured using radio waves in a manner that could enable them to receive signals from all directions using omnidirectional antenna. Constant Bit Rate (CBR) traffic model with a packet size of 512 bytes and sending rate of 4 packets/second was set to handle packet traffic. The simulation time for each scenario was set to 400 seconds. The data rate between nodes was set as 200 Mbps with delay of 2 milliseconds. Finally, nodes' radio transmission range was set to a radius of 250 meters. Table 2 is a summary of the simulation parameters.

Table 2. Simulation Experiment Parameters

Parameter	Value
Channel Type	Wireless Channel
Simulation Time	400 seconds
Number of nodes	50
MAC type	IEEE 802.11
Routing Technique	RCBDT
Movement Model	Random Way Point
Traffic model	Constant Bit Rate (CBR)
Receiving Antenna	Omnidirectional Antenna
Transport layer protocol	User datagram protocol (UDP)
Radio Transmission range	250 meters
Packet size:	512 bytes
Data Rate	200 Mbps
Sending frequency	4 packets/second
Simulation Area	1500*1000
Routing Protocol	AODV, DSR, OTB-DSR
Node speed	1-10 meters/second
Number of black hole nodes	2,4,6,10

c) Simulation of the Proposed OTB-DSR Protocol

To test the effectiveness of our proposed OTB-DSR protocol, three simulation scenarios were conducted with the following energy models; 60 joules, 80 joules and 100 joules. In each simulation scenarios, six simulation experiments were conducted; data collected and the averages for each performance metric calculated. The average values for each performance metrics were then plotted using gnuplot software. The results for the different metrics used are represented in figures 6 to 9.

7. Results and Discussions

a) Packet Delivery Ratio

Table 3 shows the sample data extracted of packet delivery ratio of the three protocols. The data was extracted after the simulation process. This data was used to plot the graphs in figure 6 that depict PDR of the proposed OTB-DSR protocol compared to AODV and DSR used as benchmark protocols.

Table 3. Packet delivery Ratio

Malicious Nodes	AODV	DSR	OTB-DSR
1	84.6	87.2	95.2
2	83.2	86.9	94.6
3	82.9	85.7	94.1
4	81.6	84.9	93.7
5	80.9	83.8	92.9
6	79.5	81.6	91.9
7	77.8	80.7	90.6
8	75.7	79.8	89.2
9	74.4	79.1	88.4
10	73.3	78.6	87.8

Figure 6 is a graph of Packet Delivery Ratio against Pause Time generated during the simulation. From the graph OTB-DSR protocol has the highest PDR of 98%. DSR and AODV used as the benchmark protocols had a PDR of 79% and 76% respectively. This implies that OTB-DSR protocol had the lowest packet loss during packet delivery. This scenario is attributed to trust recommendation amongst neighbouring nodes and selection of safe source routes from the nodes cache. During packet transmission, OTB-DSR used the route selector module to establish the safest route without wasting much time as opposed to the benchmark protocols. In OTB-DSR protocol source route with the highest RTV is given the highest preference; as it's considered the safest for packet transmission. The situation minimized chances of cooperative blackhole nodes participating in the packet routing process.

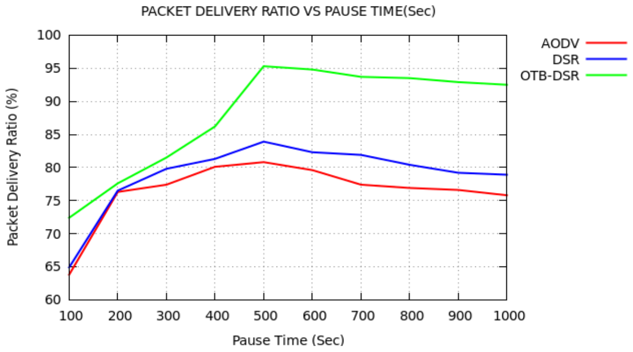

Figure 6. Packet Delivery Ratio versus Pause Time

From Figure 7 OTB-DSR protocol performed better than the benchmark protocols in the presence of cooperative blackhole nodes. The proposed protocol had a minimum PDR of 87% and a maximum PDR of 95% in the presence of two to ten blackhole nodes in the network. The benchmark protocols AODV and DSR had a minimum PDR of 73% and 78% and a maximum PDR of 84 and 87% respectively. This implies that the element of trust recommendation amongst neighbouring nodes has enabled the proposed OTB-DSR protocol lock out the malicious nodes to a greater extent during route discovery. Further, the issue of Composite Trust Values per node basis has enabled the route selector to prioritize source routes in the cache based on RTVs. This ensures that only source route with the highest RTV is given the first preference during packet transmission.

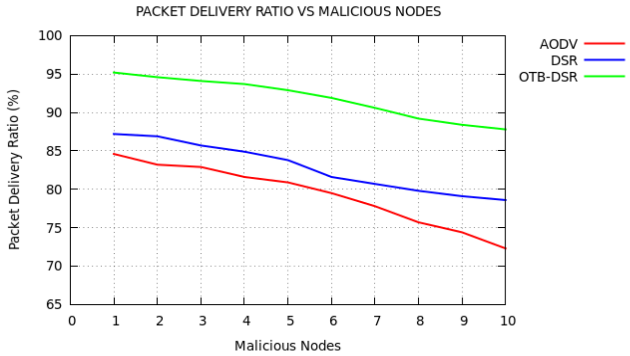

Figure 7. Packet Delivery Ratio versus Malicious Nodes

b) End-to-End Delays

Table 4 represents sample data of end-to-end delays of the three protocols. The data was extracted after the simulation runs. The data was used to plot the graphs in figure 8 that depict the end-to-end delays of the proposed OTB-DSR protocol compared to AODV and DSR used as benchmark protocols.

Table 4. End to End Delay (m/sec)

Nodes	AODV	DSR	OTB-DSR
10	2.84	2.42	1.65
15	2.62	2.18	1.54
20	2.34	1.77	1.18
25	1.98	1.46	1.13
30	1.95	1.28	0.95
35	1.86	1.17	0.93
40	1.79	1.23	0.91
45	1.82	1.15	0.92
50	1.77	1.13	0.90
55	1.76	1.14	0.91
60	1.69	1.07	0.90

Figure 8 indicates that the turn-around time of a node is high when there are a few nodes in the network. Turn-around time is the time taken between submission of a request (RREQ) and recipient of a response (RREP) by a node. Higher turn-around time translates to the higher the end-to-end delay. Simulation results indicate that on average, OTB-DSR protocol had the lowest end-to-end delays of 0.9 Seconds to 1.65 Seconds. The benchmark protocols DSR and AODV had end-to-end delays of between 1.1 Seconds to 2.4 Seconds and 1.7 Seconds to 2.9 Seconds respectively. This implies that the proposed OTB-DSR protocol has the capability of prioritizing source routes in the cache not only based on the RTV value but also on the hop counts to destination. This fact is attributed to Gratuitous Route Reply that automatically scans for trusted shorter routes to destination. In case all source routes in the cache have the same RTVs; source routes with the shortest hop counts to destination has better chances of being selected. Further, the element of trust recommendation has enabled the proposed OTB-DSR protocol to optimize effectively other route optimization techniques such as Salvaging, and Gratuitous Route Repair.

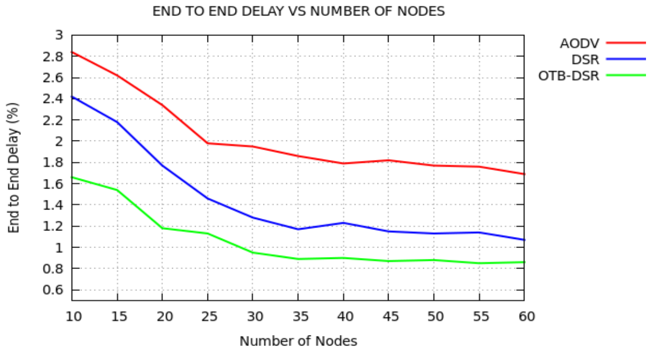

Figure 8. End-to-End Delay versus Number of Nodes

c) Routing Overhead

Table 5 represents sample data of routing overheads of the three protocols. The data was extracted after the simulation runs. This data was used to plot the graphs in figure 9 that depict the routing overhead of the proposed OTB-DSR protocol compared to the two benchmark protocols.

Table 5. Routing Overhead (%)

Malicious Nodes	AODV	DSR	OTB-DSR
10	6.1	5.3	4.75
9	5.8	4.9	4.57
8	5.35	4.5	3.94
7	5.21	4.45	3.76
6	5.1	4.3	3.51
5	4.92	4.19	3.34
4	4.89	4.03	2.97
3	4.88	3.9	2.74
2	4.65	3.73	2.56
1	4.59	3.70	2.47
0	4.57	3.68	2.32

Figure 9 shows that routing overhead increased as the number of nodes increased in the network. This is attributed to the fact that when nodes are many, a lot of control information has to be maintained. Control information aids in maintaining packet Meta data during packet transmission. The proposed protocol had a lower routing overhead compared to its benchmark protocols. OTB-DSR protocol had a maximum routing overhead of 4.75%, while the DSR and AODV used as benchmark protocols had a maximum of 5.25% and 6.1% respectively. This implies that in a transmission frame of OTB-DSR protocol, more of data packets than control packets were transmitted compared to its benchmark schemes. Further, the element of trust recommendation has reduced to greater extent issues of malicious nodes that create redundant and malformed packet which increase routing overhead. Malformed packets are larger in size than normal packets, hence occupying more storage space in a transmission frame. The purpose of malformed packets is to carry inexistent addresses that redirect or create infinite loops in transmission.

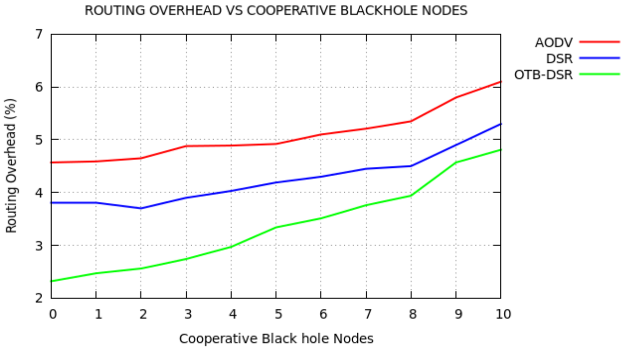

Figure 9. Routing Overhead Versus Cooperative Blackhole Nodes

d) Throughput

Throughput is the number of successful packets delivered by a network per second. It is measured in bits per second (bps). Table 6 shows the sample throughput data of our simulation. The data was extracted after the simulation runs. This data was used to plot the graphs in figure 10 that represents the throughput of the proposed OTB-DSR protocol as compared to AODV and DSR used as the benchmark protocols.

Table 6. Throughput (Kbits/sec)

Malicious Nodes	AODV	DSR	OTB-DSR
10	74	77	95.6
9	75.4	78.1	96.1
8	76.7	78.4	96.8
7	77.8	78.7	97.3
6	79.0	81	97.5
5	83.8	82.8	97.7
4	87.4	84.9	97.9
3	90.7	87.4	98.4
2	96.3	95.3	98.6
1	96.4	96.9	98.7
0	99.8	99.8	98.8

The throughput of AODV, DSR and OTB-DSR protocols in a normal scenario was 99.8 kbps; an environment with no cooperative blackhole nodes. This implies that in a normal case more packets are successfully delivered.

In the presence of cooperative blackhole nodes, the throughput drops; this is attributed to packets dropping by the malicious nodes. During the simulation, 2 to 10 blackhole nodes were introduced to the network. When 2 to 6 blackhole nodes were introduced, the throughput of OTB-DSR dropped from 99.8 to 97.5 Kbps while that of AODV and DSR dropped from 99.8 to 79 Kbps and 99.8 to 81 Kbps respectively. Further, when 7 to 10 were introduced, the throughput of OTB-DSR protocol dropped from 97.5 to 95.6 Kbps while that of AODV and DSR dropped from 79 to 74 Kbps and 81 to 77 Kbps respectively.

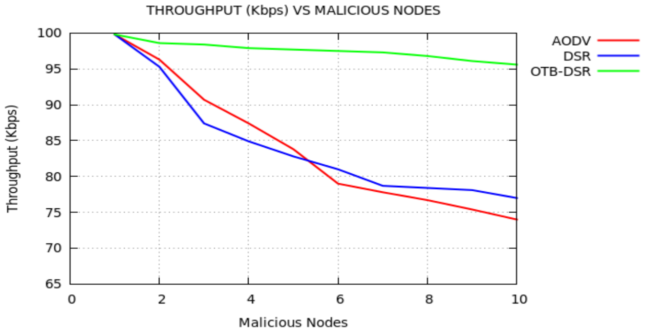

Figure 10. Throughput Versus Cooperative Black hole Nodes

8. Conclusions and Future Work

In this paper, we developed an OTB-DSR protocol by integrating dynamic trust and friendship functions in the architecture of the standard DSR protocol. The proposed protocol was simulated in NS-3 simulator. To compare the performance of OTB-DSR protocol with the benchmark protocols; Packet Delivery Ratio, Routing Overhead, End-to-End Delay and throughput were used as our performance metrics. Simulation results indicated that in terms of the four performance metrics, the proposed protocol is superior to AODV and standard DSR used as benchmark protocols. The Optimized Trust-Based DSR protocol had a packet delivery ratio of above 95%, routing overhead of about 4.75%, end-to-end delay of between 0.9 seconds and 1.65 seconds and a throughput of 95.6 Kbps, while the performance of the benchmark protocols was slightly lower.

As part of our future work, we intend to improve the proposed OTB-DSR protocol so that it can mitigate a range of active attacks such as Sybil, jelly fish, worm hole and grey hole attacks that compromise communication in MANETs.

REFERENCES

[1] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala, “A Novel Solution for Gray hole Attack in AODV Based MANETs”, In Proc. of Third International Conference on Advances in Communication, Network and Computing: Springer, February 2012. pp. 60-67.

[2] A. Boukerche, B. Turgut, N. Aydin, M. Ahmad, L. B¨ol¨oni, and D. Turgut, “Routing protocols in ad hoc networks: a survey of Computer Networks”, 2011, Vol. 55(13) pp. 3032–3080.

[3] Jeenat Sultana and Tasnuva Ahmed, “Securing AOMDV Protocol in Mobile Ad hoc Network with Elliptic Curve Cryptography”, International Conference on Electrical, Computer and Communication Engineering (ECCE), @2017,

IEEE, pp.539-543.

[4] Sagar R Deshmukh, P N Chatur and Nikhil B Bhople, “AODV-Based Secure Routing Against Black hole Attack in MANET”, IEEE International Conference on Recent Trends in Electronics Information Communication Technology, @2016, IEEE, pp.1960-1964.

[5] Soufiene Djahel, Farid Na¨ıt-abdesselam, and Zonghua Zhang, “Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges”, IEEE Communications Surveys & Tutorials, 2011.

[6] Abdelshafy M. A. and King P. J. B., “Resisting Black hole Attacks on MANETs”, 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), @IEEE 2016.

[7] Bao, F., Chen, R., Chang, M., and Cho, J.-H., “Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. Network and Service Management”, @IEEE 2012, 9, pp. 169-183.

[8] Denko, M. K., Sun, T., and Woungang, I., “Trust management in ubiquitous computing: A Bayesian approach. Computer Communications”, 2015, 34, pp. 398-406.

[9] Cho, J.-H., Swami, A., and Chen, R., “A survey on trust management for mobile ad hoc networks, Communications Surveys & Tutorials”, @IEEE 2011, 13, pp. 562-583.

[10] Abd El-Haleem, A. M., and Ali, I., A., “TRIDNT: The Trust-Based Routing Protocol with Controlled Degree of Node Selfishness for MANET”, *International Journal of Network Security & Its Applications (IJNS*A), 2011, 3(3), pp.189-204.

[11] Airehrour, D., Gutierrez, J., and Ray, S. K., “GradeTrust: A Secure Trust Based Routing Protocol For MANETs. International Telecommunication Networks and applications Conference (ITNAC), 2015, 65-70,
DOI: 10.1109/ATNAC.2015.7366790.

[12] Sultana, J., and Ahmed, T., “Securing AOMDV Protocol in Mobile Ad hoc Network with Elliptic Curve Cryptography”, IEEE International Conference on Electrical, Computer and Communication Engineering (ECCE), 2017, pp. 539-543.

[13] Sreenath N., Amuthan A., and Selvigirija P., “Countermeasures against Multicast Attacks on Enhanced-On Demand Multicast Routing Protocol in MANETs”, International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, © 2012 IEEE.

[14] Jhaveri R. H., “MR-AODV: A Solution to Mitigate Black hole and Gray hole Attacks in AODV Based MANETs”, 3rd International Conference on Advanced Computing & Communication Technologies. © 2013 IEEE,
DOI 10.1109/ACCT.2013.6, pp. 254-260.

[15] Gupta S. and Woungang I., ”Trust-Based Security Protocol against Black hole Attacks in Opportunistic Networks”, 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), © 2013 IEEE, pp. 724-729.

[16] Arya N., singh U. and singh S, “Detecting and Avoiding of Worm Hole Attack and Collaborative Black hole attack on MANET using Trusted AODV Routing Algorithm”, IEEE International Conference on Computer, Communication and Control (IC4-2015), 2015, pp. 205-210.

[17] Woungang I., Dhurandher S. K., Peddi R. D., and Obaidat M. S., “Detecting Blackhole Attacks on DSR-based Mobile Ad Hoc Networks”, © 2012 IEEE. pp. 102-107.

[18] NS-3 (version 3.25), https://www.nsnam.org (accessed 30 November 2019).

[19] NS3 official website, https://www.nsnam.org/ (accessed 24 January 2020).

[20] Shankaran, R., Varadharajan, V., Orgun, M. A., and Hitchens, M., “Context aware trust management for peer-to-peer mobile ad-hoc networks”, *Presented in 33rd Annual IEEE International Conference in Computer Software and Applications*, 2009 2, 188-193.

[21] Jain, A., Prajapati, U., and Chouhan, P., “Trust based mechanism with AODV protocol for prevention of black-hole attack in MANET scenario”, *In Proceedings of the 2016 Symposium on Colossal Data Analysis and Networking, CDAN 2016, Indore, India*.