# TRUST BASED SECURITY MODEL TO WITHSTAND AGAINST BLACK HOLE AND GREY HOLE ATTACKS IN MILITARY BASED MOBILE AD HOC NETWORKS

S.Sivagurunathan[1] and K.Prathapchandran[2]
Department of Computer Science and Applications
Gandhigram Rural Institute-Deemed University, Gandhigram-624 302
Tamilnadu, India

***ABSTRACT***

*Significant features of Mobile Ad Hoc Networks make it suitable for modern military communication. These characteristics also weaken the security aspects in terms of attacks. Among the attacks, black hole and grey hole attacks are notable since they are launched internally and cannot be identified easily. The military communication requires confidential information sharing, ensuring correct identity of soldiers but offering such facility in military based MANET is difficult due to its unique nature. As providing authentication is a first form of security, in this article we propose a trust based security model to identifying black hole and grey hole nodes that weaken or collapse the success of mission in military communication. To provide authentication, we incorporate soldier's interpersonal characteristics in terms of Stereo trust, Situational Awareness trust and soldier's operational things in terms of first-hand information, second hand information and soldier's current trust. Simulation results show the efficiency of our proposed model in terms of identifying black hole and grey hole nodes and its performances are compared with an existing model.*

***KEYWORDS***

*Mobile Ad hoc Networks, Authentication, Security, Black hole, Grey hole, direct trust, indirect trust,, Situational Awareness, Stereo.*

## 1. INTRODUCTION

Mobile Ad hoc Network also known as MANET is a collection of autonomous mobile nodes that are connecting together in a self-organized manner over a wireless medium. Mobile nodes, also lead to dynamic topology. Due to limited wireless range, it is multi-hop in nature so that it follows the peer to peer communication mechanism. Due to distributed nature there is no central control; therefore every node depends on other nodes for forwarding and act as routers. Such distinct characters make MANET differ from other networks and support many applications that run on top of it. Military is one such application and makes use of MANET as a core communication technology. The success of an application depends on how it is secure likewise the success of a military environment also depends on how it is secured. As mobile communication plays a vital role, their security is also in focus. Military application differs from commercial applications in two ways one is military environments are subject to obvious threats that are not subject to restriction protocols and another one is failures of a technology to perform can exert a cost in terms of loss of life [1]. Hence applying a technology like MANET in a highly sensitive application like military environment is always notable in terms of their security.

DOI : 10.5121/ijmnct.2016.6101 

MANET has weakness in terms of security due to its unique nature so deploying military environment in MANET becomes highly insecure. Moreover the restriction of adversary in such environment is very low due to many factors such as weakness of technology, unexpected operational conditions, and lack of cooperation among the soldiers, lack of communication and so on. In general in a military environment, soldiers are working together to achieve a mission and they assume that all are performing well. But in practice it is not true due to attacks. The attacks are launched due to poor physical protection in military environment, open and lack of centralized control, due to resource constrained military equipment, limited bandwidth of wireless devices and so on. The notable and most dangerous attack are black hole [2] [3] and grey hole attacks [4] [5] since they are harder to detect and launched internally because of overload, congestion and selfish nature of nodes in the network. In black hole attack a misbehaving node claims itself to be the most suitable node to forward packets and takes advantages and sends a *RPLY* packet first without checking whether it has desired route or not to the destination. So that source node wrongly assumes that a black hole node has desired route to the destination by the way a black hole node can retain all the incoming data packets that are intended to be forward to the destination. Simply we can say that those nodes are no longer participate in the network[6] Then, grey hole attack is a variation of black hole attack where an opponent behave just like an authentic node during the initial route discovery process thereafter it drops the packets which is intended to forward even if there is no congestion. Moreover the detection of such attack is harder because an attacker behaves just like a normal node so that we can't distinguish. Simply we can say those nodes participate in route discovery process and thereafter simply drop all the incoming packets that are intended to be forward [6].

This work is the extensions of our earlier work [7] where we achieve the authentication by identifying the collaborative black hole attacks over DSR routing protocol. In this work, we investigate our proposed work against both black hole and grey hole attacks on the Dynamic Source Routing protocol (DSR) [8] so that trusted soldiers will be identified hence authentication are achieved. The remainder of this paper is organized as follows section 2 discussed the need for authentication and trust in military scenario, section 3 discusses the brief explanation of DSR routing protocol and impact of grey hole and black hole attacks in military scenario over DSR routing protocol, section 4 deals with the related work, section 5 discusses the proposed work, section 6 discusses the results and discussion and finally section 7 discuss the conclusion.

## 2. NEED FOR AUTHENTICATION AND TRUST IN MILITARY SCENARIO

This section discusses the need for authentication in military based MANET. In military scenario, identification of trusted soldiers is always a major requirement so as to achieve the mission successfully but in MANET based military environment it is difficult. As mentioned earlier, the success of the mission depends on how the security requirements such as availability, integrity, confidentiality, authentication, non-repudiation, authorization and anonymity [9] are defined.
In military scenario, success of a mission depends on effective communication between the team members and the commanders hence identification of trusted team members and commanders is the requirement; that means authentication needs to be provided before communication begins. That will be achieved by evaluating the trustworthiness of entire team. Hence all soldiers and commanders must ensure the identity of their own team members.

Among the security requirements, authentication is important because authentication provides first level of security in military environment and it is defined as the ability of a node to ensure the identity to the receiver [9]. Typically authentication is carried out in two ways. The first one is initial authentication, which means all the participating devices or soldiers in the network are authentic at the time of initial network deployment so that such authentication mechanism is

called pre-authentication. The next one is called post- authentication; over a period of time; every node or soldier in the network should ensure the identity of participating nodes or soldiers [10]. In this work we concentrate on post-authentication mechanism. Once authentication is achieved, remaining security requirements such as confidentiality, integrity and non-reputation [10] can be achieved easily. To achieve authentication, shared secret, Public Key Infrastructure [PKI], digital signature and digital certificate [11] are used but these techniques are centralized, pre-determined and depend on trusted third party, thereby increasing computation power, memory and consumption of communication bandwidth and battery power but military devices have resource constrains.

To provide security with limited computational capabilities, trust comes into existence because, it offers less memory overhead, less transmission overhead and less bandwidth consumption[12]. Trust is a word which is originally derived from the social sciences. Trust is defined as "one entity (trustor) is willing to depend on another entity (trustee) [13]" or "the trustor abandons control over the actions performed by the trustee[14]". According to ad hoc networks, trust could be defined as the reliability, timeliness, and integrity of message delivery to a node's intended next hop [15].

## 3. IMPACT OF BLACK HOLE AND GREY HOLE ATTACKS OVER DSR ROUTING PROTOCOL IN MILITARY ENVIRONMENT

Information which is sharing in military environment is, highly confidential so high level of security is always requirement but achieving such security level in MANET based military is still complicated task due to its unique nature. This section deals with the impact of black hole and grey hole attacks. Attack is nothing but an assault on system security that is derived from an intelligent threat [9]. In general two types of attacks are possible in MANET such as internal attack and external Attack. Internal Attacks are very difficult to predict and detect because it may be launched by any compromised or malicious node from inside the network whereas external attack arises from outside the network. It causes more additional overhead on packets and tries to prevent the normal communication among the nodes. It is further classified into two categories such as passive attack and active attack.

Passive attack obtains information from the system that is being transferred and does not affect the system resources at any way and active attack aim is to alter the system resources and affect their performance. It makes some modification of data streams and creation of false streams routing by the way it affects the network. In our proposed work we deals with internal attack such as black and grey hole attacks. Before discussing the impact of such attacks, it is necessary to know the working principal of DSR routing protocol.

### 3.1. DSR Protocol Description and its implications

DSR is based on the concept of source routing that is the entire path is explicitly mentioned in the packet header of source. Hence intermediate nodes do not require keeping the routing information also need not updates periodically like *Hello* message in AODV. It supports both unidirectional and asymmetric links. Route Discovery and Route Maintenance phases are used to achieve reliable routing in DSR [16-18].

### 3.1.1. Route Discovery in DSR

Every node in MANET maintains route cache that is used to store all available route information. The main advantages of route cache are used to speed up the route discovery process and reduce the propagation of route request. When a node wants to transmit a packet to another node, first it will check the route for a source to the destination in its route cache. If any route is found to a destination, it forwards the packets otherwise it initiates a route discovery process by propagating *RREQ* packet to its neighbouring nodes. In the meantime of *RREQ*, a node will do some other process like sending and receiving of packets from other nodes in the network. Typically the destination node does not forward any *RREQ* because it is the intended destination. *RREG* packet contains Sender's Address, Destination Address and Unique Request ID determined by the sender. While transmitting each node appends its own identifier to the forwarding node. Duplication of *RREQ* is avoided by <*initiator address and request id* > pair. Figure.1 illustrates route discovery process in DSR.There are two probabilities that will arise when a node receives a *RREG* that is a node may be an intermediate node or it may be a destination node.

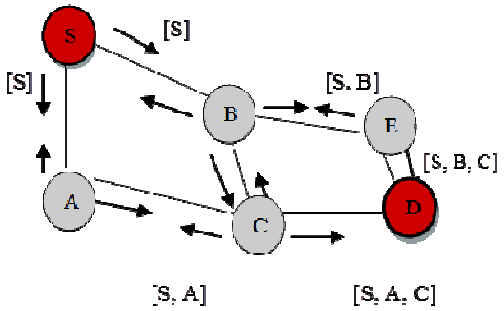


Figure 1. Route Discovery Process

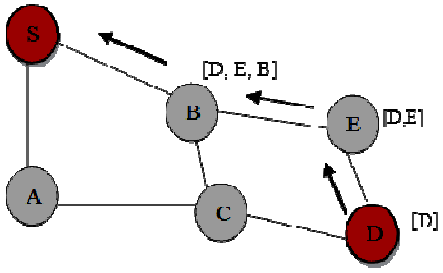


Figure 2. Route Reply Process

If it is an intermediate node, the node will perform the following actions, finding of its own address in the *RREQ* packet or if same ID of *RREQ*. In that case a node simply discards the packet otherwise the node appends its own address to the route record of the *RREG* packet and propagates to next hop neighbors. If it is a destination node, it will return a route reply message to the sender with the path where it is stored in its route cache. On receiving *RREP* the sender receives the route in route cache for subsequent uses as well as copy the accumulated route record from *RREQ* into *RPLY* here route reply is done by unicast not by multicast. Once the *RPLY* reaches the source node, the source node the actual data packet along the way to the destination. Figure.2 illustrates route reply process. When discovering a route, due to lack of route some packets may not be transmitted, those packets will be stored in the send buffer. Each packet which is stored in the send buffer will spend some specific time out period, if the packet is not delivered within that time, it will be discarded.

### 3.1.2. Route Maintenance in DSR

Route maintenance is achieved by Route Error packet (*RERR*) and acknowledgement from the receiving nodes. When error packet is received from a particular node, the entire routes of the affected node are removed from the route cache of the rest of the nodes. Acknowledgement is achieved by listening to the transmission of active nodes within the network. To ensure this appending a acknowledge bit explicitly is done. If a node fails to receive the bit, it invokes a route discovery process again by sending a route error packet to the sender.

### 3.1.3. Optimizations in DSR

**Route Reply Storms*:*** While discovering a route by *RREQ*, it is possible to receive more than one Route Reply (*RPLY*) to a requested node simultaneously from different nodes, because they have received the *RREQ* at same time. It may cause collision. This problem is called route reply storms. To avoid this, each node should randomly delay sending the route reply.

**Snooping:** At the time of processing, a node may also find some unvisited node. Those nodes' routes are also stored in the route cache. This multiple alternative nodes may be used at the time of link failure.

**Salvaging:** when a node finds a route established to a particular destination node is broken hence it generates *RERR* to its upstream node and search if there are any alternative routes in its route cache. If found the node modifies the route as per the route cache and forwards it to next hop node.

**Route Shortening:** Node *S* wants to route a packet to Destination *D* via some intermediate nodes called *A* and *B* hence the path is *S-A-B-D*. In this case node *B* sends a gratuitous massage to Node *S* that has a path to *D*. So instead of using the path *S-A-B-D*. Node S uses *S-B-D* because Node *B* has a route to *D*.

**Spreading of Route Error Messages:** When a node receives a *RERR* message for the *RREQ*. It piggybacks the *RERR* on a new *RREQ* to its neighboring nodes. It will awake nodes to update their route cache to avoid the stale routes in *RPLY* sent by the neighbors.

**Hop Limits:** Each node has a field called hop limit, it shows the propagation of *RREQ* to the number of hops (i.e.) how many intermediate nodes are allowed to forward the *RREQ*. On receiving this, the node decrements the hop limit by one before forwarding it. When the limit reaches zero the packet will be discarded even if it does not reach the destination.

### 3.1.4. Advantages and Disadvantages of DSR

**Advantages*:*** It is based on the concept of source routing so the intermediate nodes need not keep the routing information because the entire route information is stored in the packet header, resulting reduce in memory overhead, also there is no need of periodic update. Route caching is used to reduce the overhead of route discovery. Discovery of single *RREQ* yields multiple routes to the destination due to multiple replies from the intermediate nodes so it does not affect the propagation even if link failures occur. Reduce in overhead of route maintenance is achieved because route maintenance is done only between nodes that need to communicate.

**Disadvantages*:*** It is not suitable for large networks because if the number of nodes increase, the diameter of the network may also increase, due to this the packet header where all the available routing information to reach the destination may also increase hence will consume more bandwidth, also care is needed when collision occurs.

## 3.2 Black hole and Grey hole attacks

In DSR protocol, a node wants to send a packet to a particular destination, first it checks whether it has route to the destination in its route cache. If it has, simply uses that route for relaying the packet. Otherwise it initiates the route discovery process by using *RREQ* packet (Arrow Line). Upon receiving the route request packet *RREQ* the intermediate nodes give response by sending

the *RPLY* (Dotted Arrow line) packet back to the source if they have desired route to the requested Destination.

According to the protocol specification, DSR protocol gives response and sends data packet to the first route reply from the neighboring nodes though it receives multiple route replies. Here a black hole node takes this advantage and sends a *RPLY* packet first without checking whether it has desired route or not to the destination. So that source node wrongly assumes that a black hole node has desired route to the destination by the way a black hole node can retain all the incoming data packets that are intended to be forwarded to the destination. The Figure.3 shows the black hole where BH is a black hole node, it gives RPLY without checking whether it has desired route or not so that all the data packets that are intended to be forwarded are dropped.

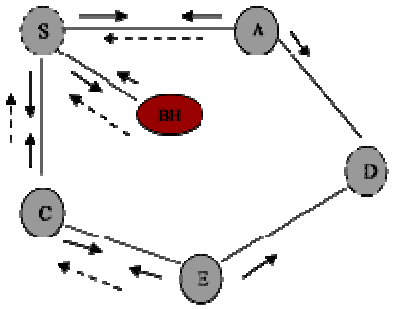


Figure 3. Black hole attack

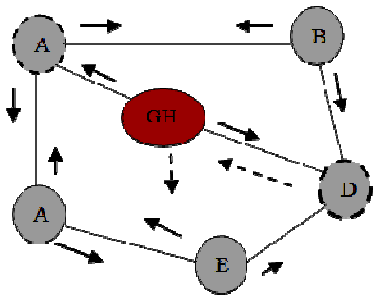


Figure 4.Grey hole attack

On the other hand, grey hole attack is simply drops the incoming packets that is intended to be forwarded to others. The Figure.4 shows the grey hole attack where GH is a grey hole node it drops the route reply (RPLY) that is forwarded by destination node D to the source node A so that all the packets that are intended to be forwarded are dropped.

In military scenario deployed MANET, to execute a mission every soldier depends on other soldiers so that they forward any mission related information via their one hop neighboring soldiers. Over a period of time, a normal node may act as a black hole node so that it does not forward any mission related information that is intended to be forwarded and if it is grey hole node, it does not forward any mission related information instead it simply drops all or partial incoming packets due to overload, congestion and selfishness. This results in mission failure and the human life becomes a question mark.

## 4. RELATED WORK

Though there exists an extensive range of literature dealing with security in MANET, only few of them focus on collaborative attacks that mainly deal with authentication. The author [16] proposed a robust and distributed access control mechanism to secure the network and encourage cooperation by excluding misbehaving nodes from the network by dividing the access control responsibility into local and global context. This model also utilizes the voting mechanism to punish the malicious nodes. The author [17] proposed a trusted based DSR routing protocol also known as TBDSR to identify the collaborative black hole attacks based on route request and forward credit. Other than this work, the authors [18] [23-26] discuss various trust based mechanisms.

The author [20] proposed prevention and elimination of gray hole attack by packet update scheme where information about the suspected nodes is fetched from neighbors. Next the author [21]

proposed a mechanism to detect collaborative grey hole attacks based on destination based scheme with consist of three phases such as store the route reply packets in pervious nodes, check the neighbors those who are all 2 hop distances of suspected node and eliminate the route reply packets from the suspected node. Other than there are so many authors [22-26] deals with the grey hole attack. Our work differs from the existing work we consider interpersonal characters of a soldier as a factor in trust assessment mechanism.

# 5. PROPOSED MODEL

## 5.1. Assumptions

We assume a pure military based MANET environment without a centralized administration. We assume that mobile devices such as handheld radio, man pack radio, laptops, cameras and Personal Digital Assistants (PDA) are carried by soldiers. All the devices are equipped with radios and embedded router that forms a pure military based MANET. We assume each soldier's walking speed range from (0 to M) meter/second where 0 denotes the lower speed and M denotes the high speed and the walk is in restricted random walk manner towards achieving a mission. At the time of initial network deployment the entire team is trustworthy and authentic and equipped with all resources. We place any number of the armed soldiers under a team and all teams are small in size. A solider can move from one team to another without the knowledge of others due to disconnection, mobility or failure of networks and also soldiers can interact with their own teammates within their transmission range.

We also assume armed soldiers are often behaving as black hole or grey hole by their inherent nature as well as environmental or operational or social conditions. We also assume military operations are executed with the support of network operations; for instance a commander wants to order a soldier to do a particular task then he makes use of underlying networking operations such as control and data packet forwarding as core factors for military commands. To execute commands from soldiers to soldiers, an underlying MANET routing protocol is required hence we make use of DSR routing protocol. Every soldier maintains a trust table where all the trust related information is stored. The trust table structure of a soldier is shown in table 1.

**Table 1.** Trust table maintained by each soldier

| Soldier ID | SAT | ST | DT | IDT | CT | OT | D | TUT |
|---|---|---|---|---|---|---|---|---|

where, ID – Soldier's identity, SAT – Situational Awareness Trust, ST- Stereo Trust, DT-Direct Trust ,IDT –Indirect trust, CT- Current Trust, OT – Overall Trust, D – Decision, TUT-Trust update time

We also assume that soldiers trust value as well as overall trust as a continuous real number in the range 0 to 1 with representation of 1 means completely trusted soldier, 0.5 means partially trusted soldier and 0 means adversaries.

## 5.2. Trust based Security Model

This section describes the proposed model over DSR protocol. Here soldier and node are interchangeable. Initially all the armed soldiers are cooperating well and trustworthy, in all level of trust related issues. Over the period of time, sensitive application like MANET based military every soldier is in situation to know about their mission that whether it is going in a right way or

wrong. Due to inherent nature of the network as pointed out earlier, every soldier is in situation to authenticate their neighbors.

Therefore according to our MTA model, over the period of time initially any soldier wants to communicate with other soldier; first he broadcasts the *Hello* packets instead of initiating route discovery process or checking their own route cache for desired route. So that a soldier ensures his one hop neighboring soldier's based on the acknowledge ultimately only one hop neighbors respond to the *Hello* packets because they are in same communication range as well as they are in active mode. Sometimes adversaries like black hole nodes also respond to *hello* packets but once a sender soldier receives response for *hello* packets and makes an entry in its trust table about the responding soldier's identity by the way a soldier can know about their own teammates. After that a sender soldier evaluates Situation Awareness Trust [27] and Stereo Trust [28] of responding soldiers and update in their Trust table. This is the initial trust assessment of a soldier about other soldiers.

The Situational Awareness Trust is assessed in person not by means of traditional network communication and it depends on individual soldiers effective communication with others by using the following factors such as, whether the soldier provides sufficient information in advance to other soldiers regarding mission execution, ability to identify operational related or equipment related threats, ability to continuously assess the situation and ability to monitor the team performance. Based on the Situational Awareness Trust, a soldier can assign rewards such as, if situational awareness trust is High, then the result is 1. If situational awareness trust is moderate then the result is 0.5. If situational awareness trust is low then the result is 0. Here the high, moderate and low values are set based on the threshold values and for each factor a reward can be assigned and finally average reward is taken, into account. Then the entry about the evaluating solider can be made in the trust table.

Next level of trust is Stereo trust, it can be assessed by a soldier about other soldier based on past experience he had in real life, hence it is purely based on local observation and information of the soldier in person. Based on the Stereo trust he can assign a reward based on threshold values. The reason behind threshold values for both situational awareness trust and stereo trust are to make trust assessment easier in terms of calculation. Therefore based on the situational aware and stereo trusts a soldier can assess the trustworthiness of other soldiers in person. Though the soldiers are good in person in the presence of other soldiers, there is a possibility for misbehave in terms of their network communication. In addition to that, we cannot apply this initial trust assessment for strangers so that we apply the next level of trust assessment based on network operations trust such as direct experience and current trust.

The direct trust of a soldier can be calculated by other soldier based on the network operations he performed during the period of time with n number of transactions and it is represented in equation 1.

$$DT_{ij} = \sum_{N=1}^{n} (\mu_1(CP_{ij}(n) + \mu_2(DP_{ij}(n)) \quad \text{where } \mu_1 + \mu_2 = 1 \quad (1)$$
$$i,j, n=1, 2, 3\ldots. \quad i \neq j$$

In the above equation DT denotes direct trust, i denote evaluating node, j denote evaluated node, CP denotes control packet forwarding ratio, DP means data packet forwarding ratio, $\mu_1$ $\mu_2$ are weighting factors. Sometimes direct trust is not enough to ensure the trustworthiness of a particular soldier hence second hand information such as opinion about others of a particular target soldier also known as in direct trust. The indirect trust is calculated based on the following equation 2.

$$IDT_{ij} = \sum_{N=1}^{n}[(\mu_1(DT_{ij}(n))* \mu_2(DT_{it}(n))] \quad \text{where } \mu_1 + \mu_2 = 1 \quad (2)$$
$$t,i,j,\ n=1, 2, 3\ldots.$$
$$t \neq j$$

where IDT denoted by indirect trust, i and t are evaluating node and j is evaluated node.

The reason for considering these packets is to check whether black hole node or grey hole is present in the network or not. Because those nodes are never forwarding the above packets that we have discussed till now. Then next level of trust is considered in terms of their current energy, closeness, co-operation with others in terms of network operations and is named as current trust of soldiers. The reason behind considering this trust is, a soldier can be involved in mission activities over a long period of time and their resource may drain quickly. Then due to lack of resource they may behave like black hole nodes. Then if two soldiers are very close in terms of their transmission range, their cooperation also increases. Hence it leads to successful mission completion. The following equation 3 is used to calculate the soldier's current trust,

$$CT = \sum_{N=1}^{n} \mu_1 \text{Co-op}(n) + \mu_2 \text{Eng}(n) + \mu_3 \text{Clo}(n) \quad (3)$$
$$\text{where } \mu_1 + \mu_2 + \mu_3 = 1,\ n=1, 2, 3\ldots.$$

From the above equation, CT denotes current trust, *Co-op* denotes cooperation, *Eng* denotes energy of the node, *Clo* denotes closeness with others.

Now a soldier can evaluate the overall trust of its evaluating soldier based on the below equation 4.

$$OT = \mu_1 SAT + \mu_2 ST + \mu_3 DT_{ij} + \mu_4 CT + \mu_5 IDT_{ij} \quad (4)$$
$$\text{where } \mu_1 + \mu_2 + \mu_3 + \mu 4 + \mu_5 = 1$$

From the above equation, OT denotes overall trust, SAT denotes Situational Awareness Trust, ST denotes Stereo trust, DT denotes direct trust, IDT denotes indirect trust and CT denotes current trust. Based on the overall trust a soldier will be able to take decision on its evaluating soldier based on the following trust interpretation table2.

**Table 2**.Interpretation of trust

| **Level** | **Trust Value** | **Soldier's Security Level** | **Notification** |
|---|---|---|---|
| 1 | If overall trust < (0.0-T1) | Untrusted Soldier | Become Black hole/Grey Hole |
| 2 | If overall trust > (T2-1) | Trusted soldier | Become Normal node |
| 3 | If overall trust == (T1-T2) | Partially trusted solider | Become neutral node |

According to the overall trust a solider, he/she categorizes the evaluating soldier into three categories namely untrusted soldier becomes black hole /Grey hole nodes, trusted soldier

becomes normal node finally partially trusted soldier becomes neutral. The information about the black hole/ grey hole node can be broadcast so that it can be identified by others and separated from the mission. Trusted soldiers can actively participate in the mission. The neutral soldiers may become either trusted or untrusted based on their future trust level.

## 6. RESULTS AND DISCUSSION

The proposed model is implemented in Network Simulator 3 (NS3). In order to evaluate our proposed model, we compare with [4] model. The following table 3 illustrates the simulation parameters that we have set for the evaluation of the proposed trust model. For all the test cases we choose the source and destination in a random fashion and simulation is performed at regular interval of times and executed for four times. In addition to that, we chose a pair of black hole nodes as well as grey hole nodes as adversaries and increase those nodes in terms of percentage like 20%, 40%, 60% and 80%. We also set the threshold values 0.65, 0.50 and 0.35 respectively for threshold value 1, threshold value 2and threshold value 3.

**Table 3.** Simulation Parameters

| System Parameters | Reflection in Real Scenario | Values Utilized |
|---|---|---|
| Number of nodes | Soldiers involved in a mission | 75 |
| Mobility Model | Soldiers can move along a zigzag line from one rescue point to another by the way rescue points are uniformly distributed over the given a treated area | RandomWaypoint MobilityModel |
| Simulation Time | Denoting the overall time of mission execution | 600sec |
| Simulation Size | Denoting the coverage area for mission operation | 1000m x 2000m |
| Protocol | Used for routing mission related information | DSR |
| Data Rate | Denoting amount of digital data moved from one mission point to another | 30720bps |
| Packet Size | Denoting the unit of data that is organized from one mission point to another | 64 byte |
| Wi-Fi standard | Soldiers arms are in ad hoc mode so that easy deployed anywhere and manged of centralized structure | 802.11b |
| Traffic | Type of data that is transmitted during the mission | UDP |
| Node Speed | Denoting the soldiers walking speed | 2m/s |
| Node Pause | There is no stop time for soldiers during the mission | 0s |
| Transmission Range | Denoting the actual amount of transmit power at radio frequency produced by the Soldiers's arm | 7.5dBm |

**Packet dropping ratio:** This metric is calculated by the difference between the total number of packets actually sent and the total number of packets actually received during the simulation. Hence the Figure.5 clearly shows that packet dropping ratio of proposed model is relatively low compared with Sukla model [4]. During the simulation the Black hole/ Grey hole nodes could be identified and isolated by using proposed model so that it shows better results.

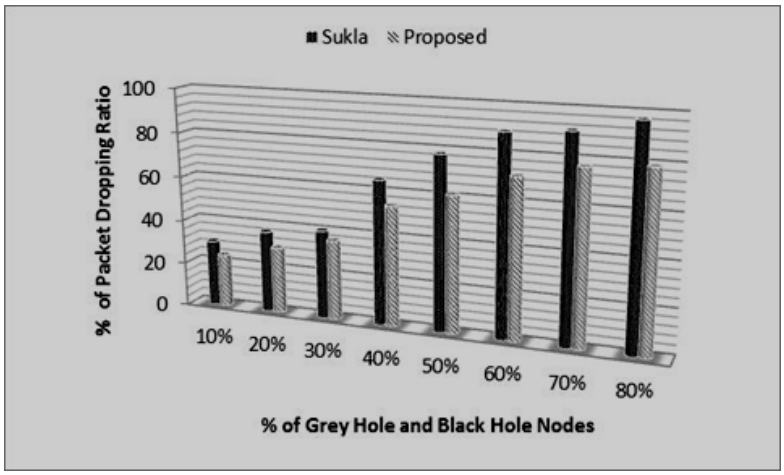


**Figure 5.** Packet dropped ratio (Sukla model [4] vs. proposed model)

**Packet delivery ratio:** This metric analyses the packet delivery ratio of each node as well as for the overall network. It is measured by the number of packets actually received divided by number of packets actually sent. The Figure. 6 depicts the packet delivery ratio of proposed is very high over Sukla model [4]because as mentioned earlier, adversaries are isolated from the network, as they are not involved in mission.

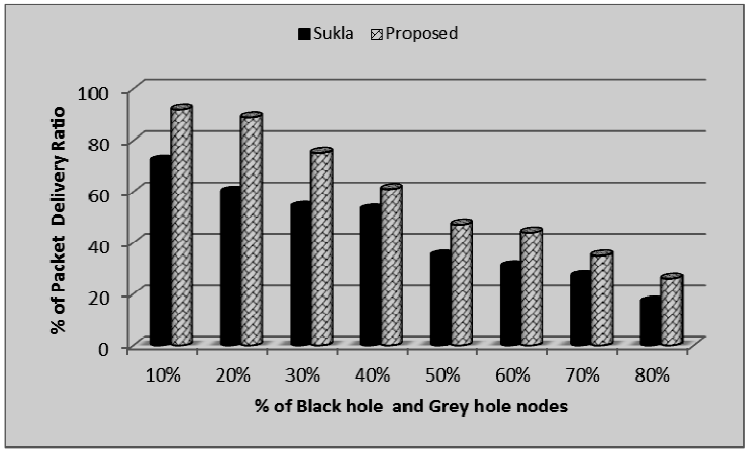


**Figure 6.** Packet Delivery ratio (Sukla model [4] vs. Proposed model)

**End to End delay:** It is measured by the average time taken by a packet from the source to the destination. Hence it is calculated by difference between the arrival time and sending time of packets from the source to the destination and the results will be divided by total number of connections between the sources to the destinations for each communication. The Figure.7 compare the end to end delay of proposed model and Sukla model [4]. From the above

performance metrics, it is clearly understood that the proposed model is better compared with Sukla model [4].

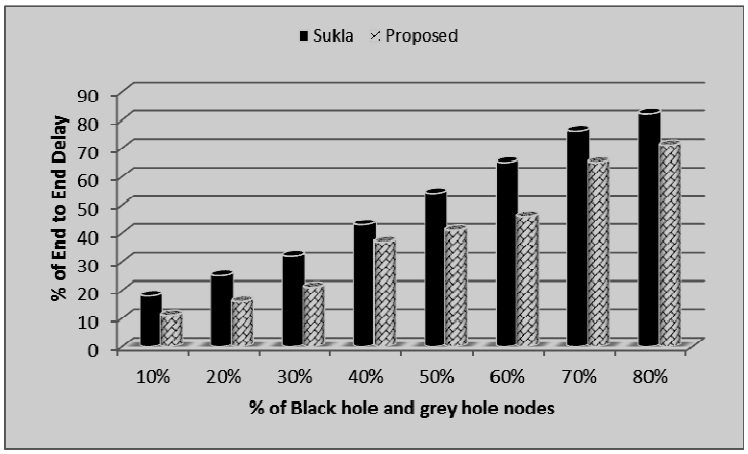


**Figure 7**. End to End delay (Sukla model [4] vs. proposed model)

## 7. CONCLUSION

In this paper we have proposed a trust based security model to identify black hole and grey hole attacks by the way authenticating of each soldier in the mission is achieved. To assess the trustworthiness of a soldier we make use of both operational factors of mission such as direct and indirect experience of soldiers and soldier's current resources that he possesses and interpersonal characters of soldiers. Moreover military equipment always possesses constrained resources so recommendation trust always leads to processing overhead. In addition to that, the proposed trust assessment is only invoked when any soldier has a doubt on his participating neighbor. So the overall network overhead is clearly less. The interpersonal character of soldiers can also affect the mission though the soldier is normal in terms of operational conditions. In future this work can be analyzed with other attacks with different routing protocols.

## ACKNOWLEDGEMENTS

This research work is supported by University Grant Commission, India, through a Major Research Project, Grant (UGC.F.No: 42-128/2013 (SR)).

## REFERENCES

[1] Brad Long, (2015), "Security Issues with the Military Use of Cellular Technology", Executive Summary accessed from www. www.ifoneinc.com on 10.11.2015.

[2] Deng H, Li W & Agrawal DP, (2002) Routing Security in Wireless Ad-hoc Networks. IEEE Communications Magazine, Vol.40, No.10, pp70–75.

[3] Fan-Hsun Tseng1 , Li-Der Chou1 & Han-Chieh Chao, (2011) "A survey of black hole attacks in wireless mobile ad hoc networks", Human-centric Computing and Information Sciences 2011, Vol.1, No.4.

[4] Sukla Banerjee, (2008) "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks", Proceedings of the World Congress on Engineering and Computer Science 2008, WCECS 2008, October 22 - 24, 2008, San Francisco, USA.

[5] V. Shanmuganathan & T.Aanand, (2012) "A Survey on Gray Hole Attack in MANET", IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), Vol.2, No.6.

[6] Michael Weeks & Gulsah Altun1, (2006), "Efficient, Secure, Dynamic Source Routing for Ad-hoc Networks", Journal of Network and Systems Management, Vol. 14, No. 4.
[7] S.Sivagurunathan & K.Prathapchandran,(2015) "Multi-dimensional trust assessment of security against cooperative black hole attacks in military based mobile ad hoc networks", Proceedings of National Conference on New Horizons in Computational Intelligence and Information System, Vol.No.1,pp344-350, ISBN.978-93-85777-02-8.
[8] Charles E.Perkins, (2001) "Ad hoc networking", Addision Wesley.
[9] William Stallings, (2003) "Cryptography and Network Security", Pearson Education.
[10] Y.Xiao, X.Shen & D.Z.Du, (2007) "Wireless Network Security", Springer.
[11] Sivagurunthan .S & Prathapchandran. K, (2014) "Trust based Security schemes in Mobile Ad Hoc Networks – A Review" 978-1-4799-3966-4/14, DOI 10.1109/ICICA.2014.67, IEEE Digital Library.
[12] Xiaoyong Li, Feng Zhou & Junping Du, (2013) "LDTS: A Lightweight and Dependable trust system for Clustered Wireless Sensor System", IEEE Transactions on information forensics and security, Vol.8, No.6.
[13] R C Mayer, J H Davis & F D Schoorman, (1995), "An Integrative Model of Organizational Trust-Academy of Management Review", Vol. 20, No.3, pp 709-734.
[14] Bamberger and Walter,(2010) "Interpersonal Trust – Attempt of a Definition", Scientific Report.
[15] Liu z, JoyA.W & Thompson R A, (2004) "A dynamic trust model for mobile ad hoc networks", proceeding of the 10 th IEEE International Workshop on Future trends of distributes computing systems, pp-80-85.
[16] Lyno Henrique G.Ferraz, Pedro B.Velloso & Otto Carlos M.B.Duarte, (2014) "An Accurate and Precise Malicious Node Exclusion Mechanism for Ad Hoc Networks," Ad Hoc Networks, Vol.19, pp142-155.
[17] Mohanapriya M & Ilango Krishnamurthi, (2013)"Trust based DSR Routing Protocol for Mitigating Cooperative Black Hole Attack in Ad Hoc Networks," Arabian journal of science and Engineering, DOI 10.1007/s 13369-013-0764-1.
[18] Kannan Govinda & Prasant Mohapatra,(2012) "Trust computations and Trust Dynamics in Mobile Ad Hoc Networks: A Survey, IEEE Communicarion surveys and tutorials, Vol.14, No.3.
[19] Liu z, JoyA.W & Thompson R A, (2004),"A Dynamic Trust model for mobile ad hoc networks," Proceeding of the 10 th IEEE International Workshop on Future trends of distributes computing systems, pp-80-85.
[20] Jin-Hee Cho, Ananthram swamia & Ing-Ray Chen, (2012) "Modeling and analysis of trust management with trust chain optimization in mobile ad hoc networks", Journal of networks and computer applications, Vol.35, pp 1002-1012.
[21] Vaishali Mittal, (2011), "Prevention and Elimination of Gray Hole Attack in Mobile Ad-Hoc Networks by Enhanced Multipath Approach", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Vol.4 No. 5.
[22] Avenash Kumar & Meenu Chawla , (2012) " Destination based group Gray hole attack detection in MANET through AODV", International Journal of Computer Science Issues, Vol. 9, No.1.
[23] Onkar V. Chandure& V. T. Gaikwad, (2011), "A Mechanism for Recognition & Eradication of Gray Hole Attack using AODV routing protocol in MANET", International Journal of Computer Science and Information Technologies, Vol. 2, No.6, pp 2607-2613.
[24] Maha Abdelhaq, (2011) "A Local Intrusion Detection Routing Security over MANET Network", International Conference on Electrical Engineering and Informatics, IEEE.
[25] R. H. Jhaveri, (2013) "MR-AODV: A Solution to Mitigate Black-hole and Gray-hole Attacks in AODV Based MANETs" Third International Conference on Advanced Computing & Communication Technologies, IEEE, pp. 254-260.
[26] S. J. Patel, (2012) "A Novel Approach to Gray-hole and Black-hole Attacks in Mobile Ad-hoc Networks" Second International Conference on Advanced Computing & Communication Technologies, 2012 IEEE, pp 556-560.
[27] Situational awareness trust (2015) access from http://www.wikipedia.com.
[28] X. lu, Anwitaman Datta & Krzysztof Rzadca, (2013) "Trust beyond reputation: A Computational trust model based on stereotypes", Electronics research and applications, Vol.12, pp.24-39.

## BIOGRAPHY

**Dr.S.Sivagurunathan** is an Assistant Professor in the Department of Computer Science and Applications, Gandhigram Rural Institute-Deemed University, Gandhigram, Tamilnadu, India. He received his B.Sc degree in Physics from Madurai Kamaraj University in the year 1995 and the M.C.A degree in Computer Applications and M.Phil degree in Computer Science from Madurai Kamaraj University, Madurai in the year 1998 and 2004 respectively. He received his Ph.D degree in Network Security from Anna University in the year 2010. He has seventeen years of experience in teaching. He is a life member of Computer Society of India (CSI). He has more than twenty publications in reputed Journals and Conferences and four publications in as book chapters. His areas of interest are Computer Networks, Mobile Ad hoc Networks, Network Security, Cloud Computing and Internet of Things. (E-Mail:svgrnth@gmail.com)

**Mr.K.Prathapchandran** is a Research Scholar in the Department of Computer Science and Applications, Gandhigram Rural Institute-Deemed University, Gandhigram, Tamilnadu, India. He received his B.C.A degree in Computer Applications from Madurai Kamaraj University in the year 2005, the M.C.A degree from Gandhigram Rural Institute – Deemed University in the year 2008 and the M.Phil degree in Computer Science from Bharathidasan University in the year 2010. He has two years of experience in teaching. He has fifteen publications in reputed Journals as well as conference proceedings. His areas of interest are Computer Networks, Mobile Ad Hoc Networks, InternetofThings(IoT)andNetworkSecurity. (E-Mail:kprathapchandran@gmail.com))