Improved Cooperation and Trust Based Model for Data Forwarding in MANET

C.DANIEL NESA KUMAR, Ph.D-Research Scholar, Department of Computer Science, Hindusthan College of Arts and Science, Coimbatore, Tamil Nadu, India. danielnesakumar@gmail.com

Dr. V. SARAVANAN, Professor and Head, Department of Information Technology, Hindusthan College of Arts and Science, Coimbatore, Tamil Nadu, India. vsreesaran@gmail.com

Abstract - Mobile Ad hoc NETwork is a cooperative network in which each node is accountable for routing and transmitting and the result consumes much battery power and bandwidth. In order to keep itself in terms of battery power and bandwidth noncooperation is legitimate. Cooperation can be improved according to the reduction in resource consumption by connecting a limited number of nodes in routing activities rather than all. The previous work designed a Backbone Group (BG) model which involves the small number of nodes instead of all. A BG is a minimal set of nodes that efficiently connects the network. However it does not detect the malicious node to improve the transmission performance. To solve this problem the proposed system designed a Trust based data forwarding scheme. In this work, initially the node trust are computed and compared with the threshold value. The nodes are detected as malicious nodes while node trust values below the threshold value. Then the malicious nodes are eliminated from the network. The Cluster Heads (CH) are selected by using Firefly Algorithm (FA) based on the delay and transmission energy. The Backbone Group (BG) model is presented routing activities. Then the Manet has divided in terms of the single hop neighborhood called Locality Group (LG). The LG Consists of Cluster Head (CH), a set of Regular Nodes (RNs) and one or more Border Nodes (BNs). The CHs are accountable for the formation and management of LG and BG. The CHs use a BG for a threshold time then switches to another BG. The experimental results show that the proposed system achieves better performance compared with the existing system in terms of throughput, energy consumption and end to end delay.

Keywords: Mobile Ad hoc NETwork (MANET), Cluster Heads (CH), Backbone Group (BG) and node Trust

I. INTRODUCTION

Mobile Ad hoc NETwork (MANET) (MANET) is an accumulation of mobile nodes furnished with both a remote transmitter and a beneficiary that speak with each other through bidirectional remote connections either straightforwardly or in a roundabout way [1]. MANET structure may change contingent upon its application from a little, static system that is profoundly control obliged to an expansive scale, portable, very powerful system. Each node works both a transmitter and a beneficiary [2]. Nodes communicate directly with each other when they are both inside a similar correspondence go. Else, they depend on their neighbors to hand-off messages.

Modern remote access and control by means of remote systems are ending up increasingly famous nowadays. One of the real favorable circumstances of remote systems is its capacity to permit information correspondence between various gatherings and still keep up their portability. This correspondence is constrained to the scope of transmitters. This implies two nodes can't speak with each other when the distance between the two nodes is past the correspondence scope of their own. MANET takes care of this issue by allowing intermediate nodes to rely data transmission. There are two kinds of MANETs: closed and open.

MANET routing protocols can be sorted into various classes as: table-driven/proactive, on request driven/receptive &hybrid. Routing protocols assume essential part in deciding execution parameters, for example, parcel conveyance division, end to (end 2 end) delay, bundle misfortune and so on of any impromptu correspondence organize .Depending on the directing topology .Proactive conventions are commonly table-driven. Cases of this compose incorporate Destination Sequence Distance Vector (DSDV). Reactive or source--started on-contingent upon the directing topology. Responsive or source-started on-request conventions don't

 DOI : 10.18231/2454-9150.2018.0411

occasionally adjust the steering data [3]-[4]. It is transmitted to the hubs just when fundamental. For Example, Dynamic Source Routing (DSR) and Ad Hoc On-Demand Distance Vector (AODV). Half and half conventions make utilization of both receptive and proactive systems. Case of this compose incorporates Zone Routing Protocol (ZRP)

Interruption is any arrangement of activities that endeavor to involve the uprightness, privacy or accessibility and an interruption recognition framework (IDS) is a gadget or programming application that screens organize movement and if any suspicious action discovered then it cautions the framework or system manager [5]. There are three principle modules of IDS are Monitoring, Analyses, Response. The Monitoring Module is in charge of controlling the gathering of information. Examinations Module is in charge of choosing if the gathered information showed as an interruption or not. Reaction Module is in charge of oversee and utilizing the reaction activities to the interruption.

Due to the limitations of most MANET routing protocols, nodes in MANETs assume that other nodes always cooperate with each other to relay data. This assumption leaves the attackers with the opportunities to achieve significant impact on the network with just one or two compromised nodes. To overcome this problem, intrusion-detection system (IDS) should be added to enhance the security level of MANETs [6]-[7]. If MANET knows how to the detect the attackers as soon as they enters in the network, we will able to completely remove the potential damages caused by compromised nodes at the first time. IDS usually acts as the second layers in MANETs. and it is a great complement to exiting proactive approaches. So intrusion detection system is very important aspect of defending the cyber infrastructure from attackers

II. LITERATURE SURVEY

In June 2008 Ningrinla marching and Raja Datta designed "collective procedure for Intrusion discovery in MANET"[8]. In this, they designed two interruption identification systems for portable specially appointed systems, which utilize community oriented endeavors of nodes in an area to identify a malignant node in that area. The first technique is designed for detection of malicious nodes in a neighborhood of nodes in which each pair of nodes in the neighborhood are within radio range of each other. Such a neighborhood of nodes is known as a clique. The second procedure is intended for discovery of vindictive nodes in an area of nodes, in which each match of nodes may not be in radio scope of each other but rather where there is a node among them which has the various nodes in its one-jump region. The two strategies utilize message going between the nodes. A node called the monitor node initiates the detection process. In view of the messages that it gets amid the recognition procedure, every node decides the hubs it suspects to be malevolent and send votes to the screen hub. The screen node after examining the votes decides the malevolent nodes from among the presumed nodes. Their IDS is free of any directing convention

N. Nasser and Y. Chen, [9] 2007, Proposed as, Many intrusion detection frameworks have been designed and the greater part of them are firmly identified with steering conventions, for example, Watchdog/Pathrater and Routeguard. These arrangements incorporate two sections: intrusion identification (Watchdog) and reaction (Pathrater and Routeguard). watch dog dwells in every hub and depends on catching. Through catching, every node can distinguish the malevolent activity of its neighbors and report different nodes. Be that as it may, if the hub that is catching and announcing itself is malignant, at that point it can cause genuine effect on arrange execution. So they designed overcome the shortcoming of Watchdog and present our interruption location framework called ExWatchdog. The fundamental element of the framework is its capacity to find pernicious hubs which can parcel the system by erroneously revealing different nodes as getting out of hand and after that returns to ensure the system. However it doesn't expand the throughput clearly

J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, [10] 2004, designed as, organize intrusion detection (ID) instruments that depend upon bundle snooping to identify distorted conduct in portable specially appointed systems. their expansions, which are relevant to a few portable, specially appointed directing conventions, offer two reaction components, detached - to uniquely decide whether a node is meddling and act to shield itself from assaults, or dynamic - to cooperatively decide whether a node, is nosy and act to ensure the greater part of the hubs of an impromptu group. They executed their expansions utilizing the GloMoSim test system and detail their viability under an assortment of operational conditions.

N. Kang, E. Shakshuki, and T. Sheltami, [11] 2010, designed as, There has been a huge development in the utilization of remote correspondence in the previous couple of decades. MANET, Its one of a kind framework less system and self-arranging ability makes it perfect for some mission basic applications, including military utilize and remote investigation. In any case, these attributes additionally make MANET powerless against latent and dynamic assaults because of its open medium, changing topology and absence of incorporated observing. To address the new security challenges, Intrusion Detection System (IDS) is required to recognize the pernicious aggressors previously they can achieve any huge harms to the system. Numerous current IDSs for MANETs depend on Watchdog instrument. In this work designed another IDS called Enhanced Adaptive Acknowledgment (EAACK) that takes care of four noteworthy issues of Watchdog component, which are vague impacts,

 DOI : 10.18231/2454-9150.2018.0411

beneficiary crashes, constrained transmission control and false trouble making report.

Kachriski and Guha [12] designed an intrusion detection system work for impromptu systems in view of versatile operators, where chosen nodes are encouraged with sensors to gather and union review information actualizing an agreeable location calculation which lessens asset utilization. The choice of these nodes depends on their network record and the result of a circulated voting calculation. Two unique strategies for basic leadership for versatile operators are designed: independent and collaborative. The utilization of community oriented approach is better as free approach may prompt single purpose of disappointment. Utilization of versatile specialists gives better adaptability as they transport their execution and state data between various sensor hosts of the system, lastly come back to the originator have with the outcome.

III. PROPOSED METHODOLOGY

A mobile ad hoc network is a self-organized network that works without any fixed infrastructure or access point. Attacks and misbehaviors are the wall that obstructs the growth and implementation.

3.1 Trust computation scheme

Direct trust can be performed by using the following derivation. Node x want to calculate the trust value on node y termed as

$$dt_{xy} = p_s / p_r \quad (1)$$

Where dt_{xy} is the final direct trust value of x and y
p_s is the successful packet sent from the node x
p_r is the successful packet receive from the node y

To calculate the direct trust, the node y, node x has to be monitors. If the trust value of the nodes is below threshold range it can be considered as malicious and eliminated from the network.

3.2. Phases of the BG Model

The designed model contains two stages i.e. the Custer head determination and Locality Group creation stage and the Backbone creation stage.

1. Cluster head selection

In this work the Cluster Head (CH) are selected by using Firefly Algorithm (FA). Here path delay and transmission energy are considered as an objective function. The parameters are calculated based on the weight basis and P denotes the path delay, E_t denotes the transmission energy.

$$F_i = W_1 * P + W_2 * E_t \quad (2)$$

Minimize Delay,

$$De_p = \sum_{(i,j)\in E} de_{ij} x_{ij} \quad (3)$$

Minimize transmission energy $E_{tx} = \sum_{(i,j)\in E} E_{tx_{ij}} x_{ij}$ (4)

de_{ij} is delay between node (i,j)

E_{tx} is transmission energy between node (i,j)

The algorithm is inspired by the flashing behavior of fireflies at night. One of the three rules used to build the calculation is that all fireflies are unisex, which implies any firefly can be pulled in to some other brighter one. The second decide is that the shine of a firefly is resolved from the encoded target work. The last decide is that allure is specifically corresponding to shine yet diminishes with separate, and a firefly will move towards the brighter one, and if there is no brighter one, it will move arbitrarily.

In firefly calculation, there are two essential factors, which is the light force and engaging quality. Firefly is pulled in toward the other firefly that has brighter glimmer than itself. The engaging quality is depended with the light force.

The light power in this way appeal is contrarily relative with the specific separation r from the light source. In this way the light and engaging quality is diminish as the separation increment.

$$I(r) = I_0 e^{-\gamma r^2} \quad (5)$$

I = light intensity,
I_0 = light intensity at initial or original light intensity,
γ = the light absorption coefficient
r = distance between firefly *i* and *j*

Attractiveness is proportionally to the light intensity seen by the another fireflies, thus attractiveness is β

$$\beta = \beta_0 e^{-\gamma r^2} \quad (6)$$

β_0 = Attractiveness at *r* is 0

The distance between two fireflies can define using Cartesian distance

$$r_{ij} = |x_i - x_j| = \sqrt{\sum_{k=1}^{d} (x_{i,k} - x_{j,k})^2} \quad (7)$$

Firefly *i* is attracted toward the more attractive firefly *j*, the movemeunt is defined as

 DOI : 10.18231/2454-9150.2018.0411

$$\Delta x_i = \beta_0 e^{-\gamma r_{ij}^2}\left(x_j^t - x_i^t\right) + \alpha\varepsilon_i, \qquad x_i^{t+1} + \Delta x_i \quad (8)$$

In equation (4), the first term is for attraction, γ is the limitation when the value is tend to zero or too large.

In this work, number of nodes are considered as fireflies and, the path delay and transmission energy is considered as an objective function.

Modified Firefly algorithm

1. Produce initial population of fireflies (number of nodes) x_i (i=1,2,...n)
2. Compute light intensity (objective such as delay and transmission energy) of fireflies
3. Describe light absorption coefficient γ
4. While(t>Max Generation)
5. for i=1:n all n fireflies
6. for j=1:i all n fireflies
7. Light intensity Ii at xi is identified
8. if (Ij> Ii) (Objective function such as delay and transmission energy)
9. Move firefly i in the direction of j in all d dimensions
10. Else
11. Move firefly i arbitrarily
12. End If
13. Attractiveness modifies with distance r via exp[-γr2]
14. Identify novel solutions and revise light intensity
15. . End for j
16. End for i
17. Rank the fireflies and identify the present best
18. end while
19. Post process outcomes and visualization

Finally based on the objective function the CH nodes are selected. In this work presented the Backbone Group (BG) model in which least number of nodes takes part in directing exercises rather than all. At initial, a MANET is intelligently partitioned as far as the single bounce neighborhood called locality group (LG) appeared in Fig. 1. In a LG has a cluster head (CH), set of Regular Nodes (RN) and at least one Border Nodes (BN). The CHs are in charge of the production of LGs, making of BGs, incorporation of BGs into choice table, trade of the alternative table to different CHs and determination of a BG for organize exercises. A BG is a negligible arrangement of hubs that effectively associates the system. The BG utilized as a part of system exercises by the CHs ought to be taken for a limit time, with the goal that the obligation of steering goes to all hubs of the region bunches similarly. The designed model does not expect any reachability requirements on the grounds that LGs are characterized based on single hop distance.

2. Locality Group creation stage

In this stage, an arrangement of CHs is characterized based on high computational power and battery lifetime, for instance in the war zone a cluster node could be a captain's laptop, because it has the high computational power and battery lifetime .In this work we have not talked about the choice of Cluster head, any current methods can be utilized to choose a CH. After that neighboring nodes are analyzed by cluster heads based on one hop distance to make at least one area group(s). One hop distance is figured based on the cluster head and the standard node areas .

Let CH = (p1, p2) and RN $=\sqrt{(p_1 - q_1)^2 + (p_2 - q_2)^2}$ (9)

(q1, q2) at that point the Euclidean separation d is characterized as

On the off chance that d<=r then the node is in the scope zone of cluster head and can be taken as a territory amass part, where r signifies the correspondence run. On the off chance that a RN is inside the scope region of at least two CHs, at that point, the CHs measure the separation of a RN and offer in its neighborhood. To make a part, CHs look at the separations amongst RN and CHs. The minimum distance is the reason for choosing a RN as a part for the LG. On the off chance that CHs are at a same distance from the RN then RN is added to any of the LGs.

Each locality group consists of a set of regular nodes, one or more border nodes under the control of one cluster head. The designed locality group has one cluster head, a set of regular nodes and one or more border nodes. The backbone group is defined by selecting a minimal set of nodes that efficiently connects the network. The regular nodes that are member of a BG is called border nodes. Fig. 1 shows that nodes of a locality group are arranged in grid pattern but we can use any other pattern as per the requirement and communication range. It also shows that a cluster node of a LG is defined at the center but it could be in the corner or periphery of the network. However, choosing a cluster node at the center covers a large geographical distance.

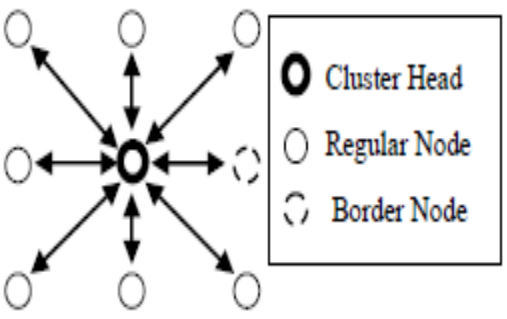


Fig. 1. Locality group

 DOI : 10.18231/2454-9150.2018.0411

Similarly, on that basis several locality groups are defined. The dotted lines show the backbone link and the dotted circle denotes the member of the BGs called border nodes. We have taken these two patterns to divide a network into locality groups, but it can be arranged in many ways as per the requirements.

3.3 Backbone creation phase

In a MANET we have n number of nodes which is divided into k number of LGs. The problem is to choose m number of nodes from each LG such that the maximum numbers of LGs are covered, i.e. the union of the selected nodes has maximal size up to the number of LGs and each LG are covered. The problem can be modeled as20: Let the MANET of size n is divided into k number of locality groups L = {L1, L2, … , Lk}

Objective is to find a subset C $\sqsubseteq$ L having m number of nodes from each LGs, such that C <= m

The problem can be formulated in linear programming problem as Maximize the sum of covered nodes from each LG such that|C|$\leq$m

$$| \ L_i \in C L_i \ | \text{ is minimized}$$

The problem can be formulated in linear programming problem as Maximize the sum of covered nodes from each LG

$$\text{Max} \sum_{L_i \in C} L_i \quad (10)$$

subject to

Select a maximum of m number of nodes from each LG

$$\sum C_i \leq m \quad (11)$$

The above problem can be solved using any greedy approach methods. In this work we have not focused on the approximation of the maximum coverage problem, here emphasis is given on backbone construction to reduce energy consumption.

3.4 Working of the BG Model

The CHs is responsible for the creation of LGs, creation of BGs, inclusion of BGs into option table, exchange of the option table to other CHs and selection of a BG for network activities. The BG used in network activities by the CHs should be taken for a threshold time, so that the responsibility of routing goes to all nodes of the locality group equally. The proposed BG model working algorithm is defined as follows.

1: Node initialization
2: trust computation
3: malicious node detection
4: Custer Head Selection
Select k number of cluster nodes using existing algorithms
5: [Locality Group creation phase]
(a) Divide the MANET into k locality groups on the basis of CH location.
(b) Include nodes within a locality group using

$$d(CH, RN) = \sqrt{(p_1 - q_1)^2 + (p_2 - q_2)^2}$$

6: [Backbone creation phase]
(a) Create BGs by solving the linear programming problem discussed in section 3.3.
(b) Add BGs into option table.
(c) Share option table to other CHs.
7: [Execution phase]
Start network operations on the basis of BG.

IV. EXPERIMENTAL RESULTS

This part explains the experimentation tools setup and parameters utilized in simulation of a MANET. Ubuntu 11 is utilized as the operating system because it is an easy to use and that makes it simple to run. Network Simulation 2 (NS2.35) is utilized as simulation software that performs effortlessly over Ubuntu 0. The proposed Trust Based data forwarding approach is compared with the existing BG based data forwarding approach in terms of End to End Delay, Energy Consumption and Throughput.

1. End to end delay

The time taken by a packet to transmit from source to destination across the network is well-known as End to End delay.

$$\text{End to end delay} = \frac{\text{Packet transmission from source to destination}}{\text{Time}} \quad (12)$$

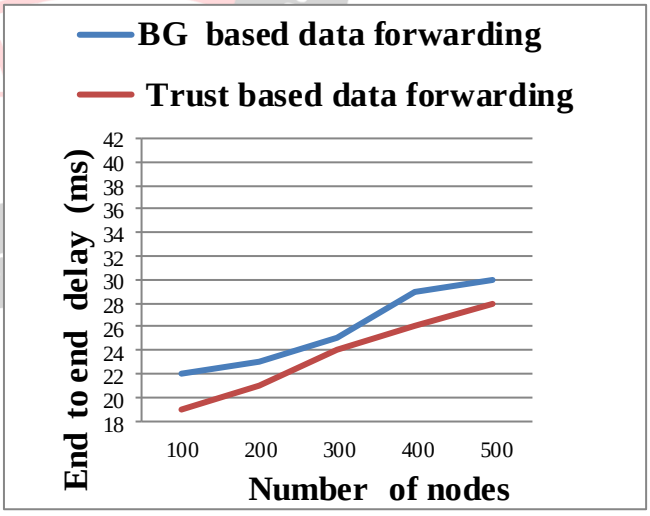


Figure 2: End to end delay comparison for 500 nodes

End to end delay performance of the proposed trust based data forwarding and the existing BG based data forwarding scheme for 500 nodes are shown in figure 2. In X axis number of nodes is taken and in Y axis end to end delay is taken. The experimental results show that the proposed system achieves lower end to end delay compared with the existing system.

 DOI : 10.18231/2454-9150.2018.0411

2. Energy consumption

The power consumption is computed by dividing the energy per packet by the transmission time per packet.

$$\text{Energy consumption} = \frac{\text{Transmisssion energy per packet}}{\text{Transmission time per packet}} \quad (13)$$

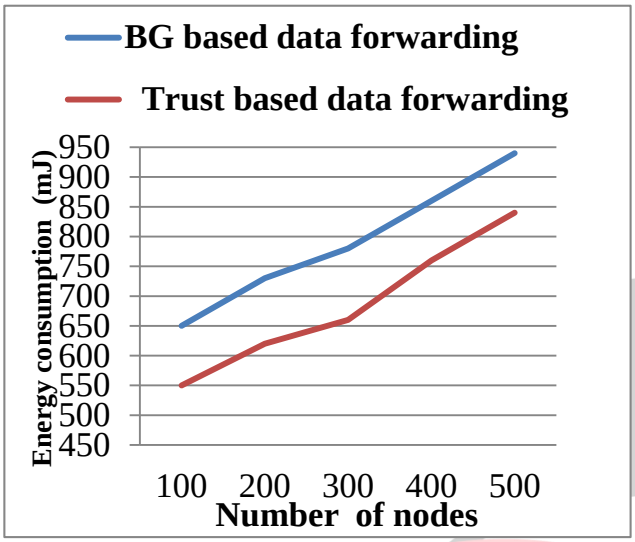


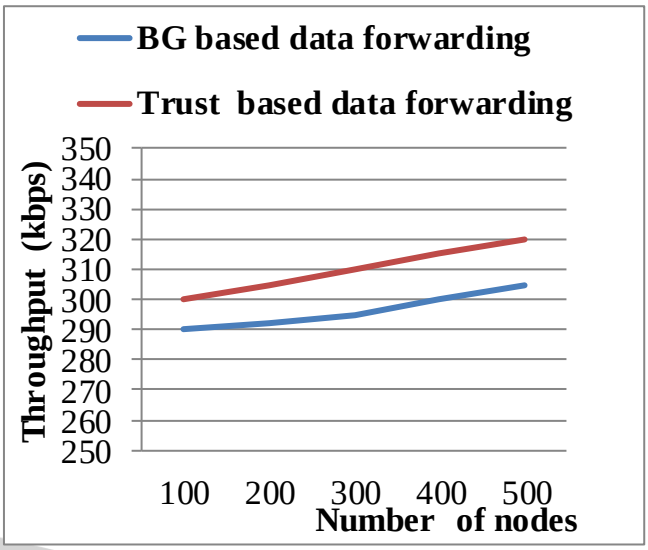
Figure 3: Energy consumption for 500 nodes

Figure 3 shows the comparison of energy consumption performance for 500 nodes. The existing BG based data forwarding and the proposed Trust based data forwarding schemes are compared. In X axis number of nodes is taken and in Y axis energy consumption is taken. The designed system provides a Firefly Algorithm (FA) algorithm for cluster head selection. From the graph it is clear that the proposed trust based data forwarding provides lower energy consumption than existing method.

Throughput

Throughput is the rate of successfully delivered data packets per second in the network between sources to destination. It is measured in bits per second (bit/s or bps). It is also specified by units of information processed over a given time slot.

$$\text{Throughput} = \frac{\text{successfully delivered data packets}}{\text{Time}} \quad (14)$$



. **Figure 4 :Throughput comparisons for 500 nodes**

Figure 4 shows that the system throughput increases along with the increases of time because the trust model. The existing BG based data forwarding and the proposed Trust based data forwarding schemes are executed for 500 nodes. In X axis, number of nodes is taken and in Y axis Throughput is taken. The experimental results show that the proposed system achieves better performance for 500 nodes compared to the existing system.

V. CONCLUSION

The designed forceful and protected system not only protects the network from attacks and misbehavior but it must devour minimum resources to extend the life of the network, and this was the basis for MANET. The proposed trust based data forwarding model enhance cooperation in MANET by connecting a minimum number of nodes (BG nodes) in routing behavior instead of all. Initially the trust value of the nodes are computed and based on that values the nodes are detected whether it is malicious or not. Once the nodes are detected as malicious removed from the network and CH is selected by using FA. In a LG the system has a cluster head (CH), a set of regular nodes (RN) and one or more border nodes (BN). The CHs are accountable for the formation of LGs, formation of BGs, addition of BGs into option table, swap of the option table to other CHs and selection of a BG for network activities. The experimental results show that the proposed system achieves better performance compared with the existing system in terms of throughput , energy consumption and end to end delay.

REFERENCES

[1] Norsuzila Yaaco, Nurhazwani Rosli, Azita Laily Yusof, Mohd Tarmizi Ali, (2013), "Investigate the Performance metrics of Mobile Adhoc Networks (MANET)," International Symposium Wireless Technology and Application (ISWTA), IEEE Computer Society, pp. 22-25.

[2] C. E. Perkins, E. M. Royer., (1999), "Ad-hoc OnDemand Distance Vector Routing," Proc. of 2nd International

 DOI : 10.18231/2454-9150.2018.0411

Conference on Mobile Computing System and Applications, IEEE Computer Society, New Orleans, LA, pp. 90-100.

[3] Elizabeth M. Royer, Charles E. Perkins, (2000), "An Implementation Study of the AODV Routing Protocol," Proc. of International Conference on Wireless Communication and Networking, (Volume: 3).

[4] Jiao wen-cheng, PENG Jing, ZHENG, (2010), "Research and Improvement of AODV Protocol in Adhoc Network," Proc. of 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM), IEEE Computer Society,pp.23 – 28.

[5] H. Yang, J. Shu, X. Meng, and S. Lu, "SCAN: Self-Organized Network-Layer Security in Mobile Ad Hoc Networks", (2006), IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, pp. 261- 273.

[6] E.Padilla, N.Aschenbruck, P.Martini, M.Jahnke and J.Tolle, "Detecting Black Hole Attack in Tactical MANETs using Topology Graph", (2007), Proceedings of IEEE Conference on Local Computer Networks.

[7] N.Ye, X.Li, Q.Chen, M.Emran and M.Xu, "Probabilistic Techniques for Intrusion Detection Based on Computer Audit Data", (2001) IEEE Transactions on Systems, Man, and Cybernetics, Vol. 31, No. 4, July.

[8] Ningrinla Marching and Raja Datta "Collaborative Technique for Intrusion Detection in Mobile Ad hoc Network" Ad hoc Networks, 6, Issue 4, June 2008 Page 508-523. [11] R.Ranjana

[9] N. Nasser and Y. Chen, "Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network," in Proc. IEEE 2007.

[10] J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, "On intrusion detection and response for mobile ad hoc networks," in Proc. IEEE 2004

[11] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in Proc.2010

[12] O. Kachirski, R. Guha, "Effective intrusion detection using multiple sensors in wireless ad hoc networks", Proc. of the 36th Hawaii International Conference on System Sciences (HICSS'03), IEEE, 2002

 DOI : 10.18231/2454-9150.2018.0411