Volume 6, Issue 10, October 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# Detection of Flood Attack using Smart Grading of Trust Factors in MANET

**Sofi Mohd Amin**
M.tech -CSE, SVIET (Banur), P.T.U
Punjab, India

**Er. Amritpal Kaur**
AP CSE, SVIET
Punjab, India

***Abstract— Mobile ad-hoc networks are widely used because these are very easy to deploy. However, there are various security issues and problems. It is effective in providing secure routing by isolating malicious nodes and other overheads from MANETs. According to the behaviours of sensor nodes, a variety of trust factors and coefficients related to the network application are established to obtain direct and indirect trust values through calculating weighted average of trust factors. Trust management is fundamental to identify malicious, selfish and compromised nodes which have been authenticated. In this paper we have studied the old grade trust scheme in order to detect the malicious attacker causing hello flood attacks in the network. We have modified the old Grade Trust scheme that was used in to detect the malicious black hole nodes in the network. In modified scheme we worked to analyse the impact of the Hello flooding attack on the network, to modify the Grade Trust Scheme to detect the flood attacker nodes in the network, to implement the modified scheme in MATLAB and to compare the performance of the network after applying the Grade Trust scheme and in the presence of the attackers. The results of the new modified scheme shows that the new scheme is more efficient then old scheme as it has less energy consumption reduced end to end delay and maximum throughput.***

***Keywords— MANETS; Trust Factor; Throughput; End To End Delay; Attacker Nodes ;AODV ; Network Life Time.***

## I. INTRODUCTION

An Ad hoc network generally means [2]MANET (Mobile Ad hoc Network).An Ad hoc network constitutes a regrouping of a large population of portable calculating units (laptops, telephones…) inter-connected by a wireless technology, moving in an unspecified territory, forming a decentralized network, without fixed infrastructure.

In mobile ad-hoc networks, nodes act as both routers and terminals. For the lack of routing infrastructure, they have to cooperate to communicate. Cooperation at the network layer takes place at the level of routing, i.e. finding a path for a packet, and forwarding, i.e. relaying packets for other nodes. Misbehaviour means aberration from regular routing and forwarding behaviour resulting in detrimental effects on the network performance. Misbehaviour arises for several reasons. When a node is faulty its erratic behaviour can deviate from the protocol and thus produce non intentional misbehaviour. Intentional misbehaviour aims at providing an advantage for the misbehaved node. An example for an advantage gained by misbehaviour is power saved when a selfish node does not forward packets for other nodes. An advantage for a malicious node arises when misbehaviour enables it to mount an attack.

Secure communication has been always an important aspect of any networking environment. It has now become a significant challenge in MANETs. It has[4] turned out to be challenging due to its unique characteristics: unreliability of wireless links, limited physical protection of mobile nodes, dynamic topology, no certified authorization, and the deficiency of a centralized monitoring. The Hello flooding attack has become a major security concern and attracted many researchers in both the academia and industry. Consequently, a large number of security mechanisms have been proposed and many commercial products have been developed in infrastructure networks, i.e., the Internet and cellular wireless networks.

In Hello flood attacks, the attacker node upon receiving the route request messages re-broadcast the request messages to the larger portion of the network by increasing the transmission range. The nodes that receive the request messages consider them genuine and they forward the request to the destination node. When the request reaches the destination and it replies to the source node then the attacker nodes are chosen in the path. The nodes try to send the data packets to the attacker nodes considering them as genuine. The nodes have lesser transmission range than attacker, so the data does not reaches properly.

There arises a need to detect such attacks during the route request phase so that loss of data can be minimized in the network. In this paper we have studied the [5]old grade trust scheme in order to detect the malicious attacker causing hello flood attacks in the network. We have modified the old Grade Trust scheme that was used in to detect the malicious black hole nodes in the network. In modified scheme we worked to analyses the impact of the Hello flooding attack on the network, to modify the Grade Trust Scheme to detect the flood attacker nodes in the network, to implement the modified scheme in MATLAB and to compare the performance of the network after applying the Grade Trust scheme

 

and in the presence of the attackers. The results of the new modified scheme shows that the new scheme is more efficient then old scheme as it has less energy consumption reduced end to end delay and maximum throughput .The rest of the paper is structured as follows**.** Section II provides an Impact of Hello Flood Attack in Network and Its Countermeasures. Section III introduces Modified Grade Trust Scheme Section IV provides the Implementation of Modified Grade Trust scheme and algorithm for detection of flood attack. Section V we present simulation parameters used in simulating the previous work and the improved work. Finally in section VI we present our concluding remarks and future work

## II. IMPACT OF HELLO FLOOD ATTACK IN NETWORK AND ITS COUNTERMEASURES

Many techniques have been proposed in the past by different researchers to detect and prevent hello flood in MANETs. Brief descriptions of these are given below:

In [16] the authors used a cryptographic technique to prevent the hello flood attack. They assumed that any two sensors share the same secret key and every new encryption key is generated on fly during the communication. This phenomenon ensures that only reachable nodes can decrypt and verify the message and hence prevent the adversary from attacking the network. But the main drawback of this approach is that any attacker can spoof its identity and then generate attacks. A security mechanism based on signal strength and geographical information is proposed in [17] for detecting malicious nodes that launching hello flood and wormhole attack. Another Neighbour-based IDS for WSN is implemented in [18]. This algorithm is based on signals that are sent between nodes to detect hello flood attacks. This algorithm is promising since the false positive is becoming lower and the false negative becoming higher with signal strength increased with an average false positive 0.28 and average false negative 3.76 with signal strength 5dB. We will compare our work against this model later in the paper. In addition, a threshold based algorithm is proposed in [19] to defend against flooding attacks in MANET. The mobile nodes use a threshold value to check whether its neighbours are intruders or not. The following section will introduce the hello flood attacks in WSNs. In [20] the authors have proposed a security solution framework tailored to the base station for defending against DoS attack. After initial DoS detection, base station challenges clients with cryptographic puzzles to protect itself from different types of attacks. Compared with traditional puzzle schemes, they introduce a novel reputation based client puzzles, which applies a dynamic policy to adjust the puzzle difficulty for each node in terms of node's reputation value. Hence the punishment for malicious nodes becomes more and more pressing without introducing extra unnecessary burden to most normal nodes .A mechanism [21] based on signal strength and geographical information for detecting malicious nodes staging HELLO flood and wormhole attacks is presented. The idea is to compare the signal strength of a reception with its expected value, calculated using geographical information and the pre-defined transceiver specification. A protocol for disseminating information about detection of malicious nodes is also proposed. The detection rate of the solution depends on different parameters. In this proposed scheme, all transmissions in the network are subject to scrutiny: all nodes monitor all transmissions they hear. For each transmission [22]a node hears, it compares the expected and the actual signal strengths of the received signal, independently of whether it is the intended recipient of the transmission. When the difference between both is greater than a given threshold, the message is regarded as suspicious.

Each node also keeps a local table containing the "reputation" of other nodes in the system. Each entry contains the node id, the number of suspicious votes, and the number of unsuspicious votes. After checking the suspiciousness of a received message, the node updates its table accordingly: if the message is suspicious, it increases the message originator's suspicious count by one; otherwise, the unsuspicious count is increased. Note that the message's originator can be determined, given that its id is included in the message. If the message is suspicious, the node takes a further action: it disseminates this information among its neighbours.

## III. MODIFIED GRADE TRUST SCHEME

In order to detect the malicious attacker causing hello flood attacks in the network, we will modify the Grade Trust scheme that was used to detect the malicious black hole nodes in the network. The modified scheme works as follows:

The source node will first broadcast the hello messages in the network. This step is executed to categorize the nodes in the grades. The nodes upon[23] receiving the hello message will broadcast it to their neighbour nodes. Also the nodes will send information about the nodes from which the hello messages have been received .The malicious nodes upon receiving the hello messages will rebroadcast them to the larger portion of the network .When the hello messages reach the destination node, the destination node will store the following information in the trust table: Node ID: Information about the nodes from which the hello messages was received.

The destination node will calculate the number of hello messages broadcasted by a particular node in the network. For the attacker node the count of the hello messages sent will be very high .The destination node will now arrange the nodes into categories: Trusted Friends, Friends and Possible Friends. Trusted [14]friends are much more secured nodes, Friends are moderately secure and the Possible Friends are not very secured .If the nodes has forwarded the request messages in very large number, then it will downgraded to Grade 1 or Possible Friends category. If the node have forwarded lesser than the average number of messages forwarded, it will have Grade 3 or trusted friend's category. If the nodes have forwarded messages closer to the average number of requests forwarded then it will having Grade 2 or Friends category. The destination node will chose only trusted friends nodes to send the route reply message to the source node. Upon receiving the reply message the source will send data over the trusted friend's category path .The above process is diagrammatically shown below in figure 1:

 

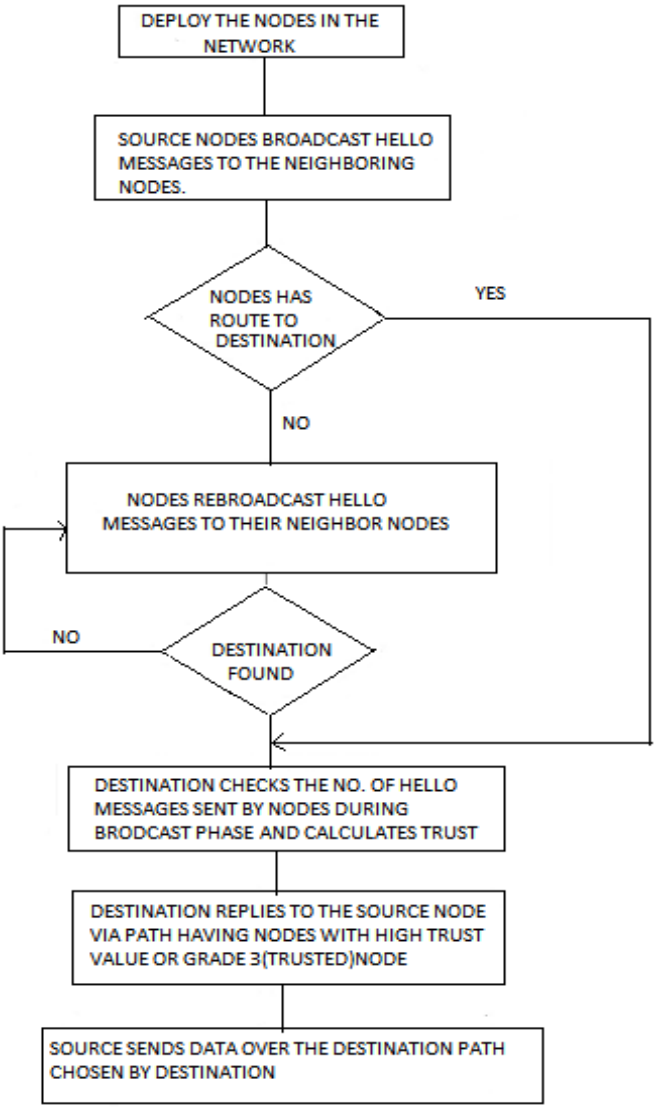


Fig.1 Logical Flow control for proposed Smart Grade Trust for detection of Hello Flood Attack.

## IV. IMPLEMENTATION OF MODIFIED GRADE TRUST SCHEME

We implement the modified grade trust scheme in MATLAB and found the results which are very effective in detecting the flood attacker nodes in the network .The Grade trust factor is given below which provides a secured trust to send request from source node to the destination node.

$$NSij = \frac{(Sij\ (1 : Avg) - Sij\ (Avg : n))}{Cij}$$

In the above equation, NSij is the trust factor, Cij is the total number of requests, Sij is the successfully forwarded requests ,Avg is the average successful forwarded requests in case of non-attack scenarios and n is the total number of successful forwarded requests . The total number of requests which is given as in the formula of grade trust factor i.e., Cij is taken as 1200.Also we will use 700 nodes in the network analysis of for the detection of flood attacks in our proposed scheme.The trust factor is computed based on below mentioned algorithm:

**ALGORITHM TO GET TRUST VALUES:**

Suppose Ni be the number of messages sent by the ith node during broadcasting phase.

Suppose M = total number of nodes.

Avg = average number of messages send by the node.

```
for i=1:M
    if Ni >> Avg
        grade = 1 ; category= P.F
        PF = (possible friend)
    end
    if  Ni < Avg
        grade = 3; category = Trusted friend
    end
```

 

```
        if  Ni = Avg
                grade = 2; category = friends
        end
end
```

In the above algorithm if the number of messages sent by the ith node during broadcasting phase is greater than the average of the grade trust factor then it will be treated as the possible friend. Also if the number of messages sent by the ith node during broadcasting phase is less than the average of the grade trust factor then it will be treated as the trusted friend and we will transfer our information through this trusted friend so that there will not be any breach of security and finally if it is equal to the average of the grade trust factor it will be treated as the friend. Based on the above algorithm, we categorise the friends on the basis of grade 1, grade 2 and grade 3. For possible friend, grade is equal to 1 and for trusted friend and friend, grade is equal to grade 3 and grade 2 respectively.

## V. THE PERFORMANCE OF THE NETWORK AFTER APPLYING THE SMART GRADE TRUST FACTOR SCHEME AND IN THE PRESENCE OF ATTACKER

The below given points provides the performance of the network after applying the Smart Grade Trust factor scheme and in presence of attackers :

### 1. Simulation of Old Scheme using Grade Trust

The figure 1 shows the simulation of old scheme which is based on grade trust scheme. In the simulation it was clearly seen that the broadcast of node is in very small range which could not easily locate the malicious black hole node in the network.

### 2. Simulation of New Proposed Scheme using Smart Grading of Trust Factor

The figure 2 shows the simulation of new proposed scheme which is based on smart grading of trust factor scheme. In new scheme the node broadcast area is maximum, using which we could easily locate the malicious black hole node in the network and can easily detect hello flood attack.

### 3. Energy consumption

The fig. 3 shows the energy graph in mille-joules of new proposed scheme which is based on grade trust scheme. By the study of graph we could conclude that the energy consumed in the previous scheme is much more than which is consumed in the new scheme.

### 4. End to End Delay

End to end delay refers to the time taken for a packet to be transmitted across a network from source to destination . The fig. 4 shows the end to end delay graph of new proposed scheme which is based on grade trust scheme. By the study of graph we could conclude that the end to end delay in the previous scheme is more than which is in the new scheme.

### 5. Throughput

Throughput is a measure of how many units of information a system can process in a given amount of time .The figure 5 shows the throughput graph in mille-seconds of new proposed scheme which is based on grade trust scheme. By the study of graph we could conclude that the throughput in the previous scheme is less than which is in the new scheme.

### 6. Network Lifetime in Rounds

The figure 6 shows the comparison of network lifetime in rounds for new proposed scheme and old scheme which are based on grade trust scheme. By the study of figure we could conclude that the network lifetime in rounds is less in previous as compared to the new scheme.

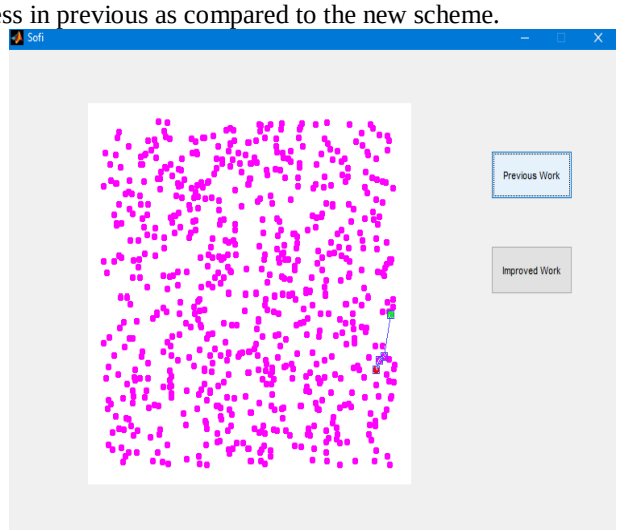


Fig. 1 Network simulation in Old scheme

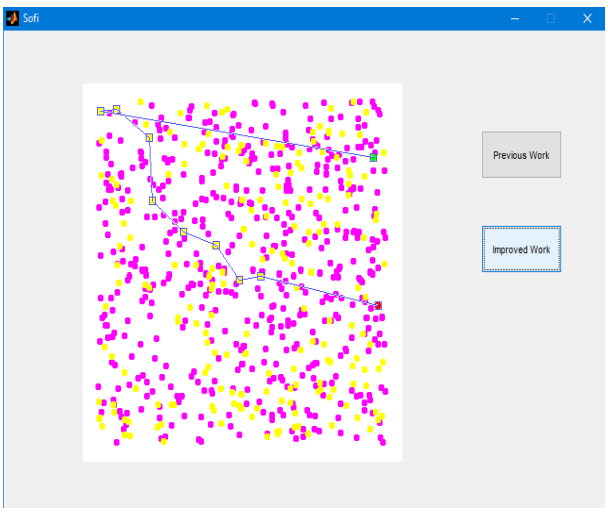


Fig. 2 Network simulation of New Scheme

 

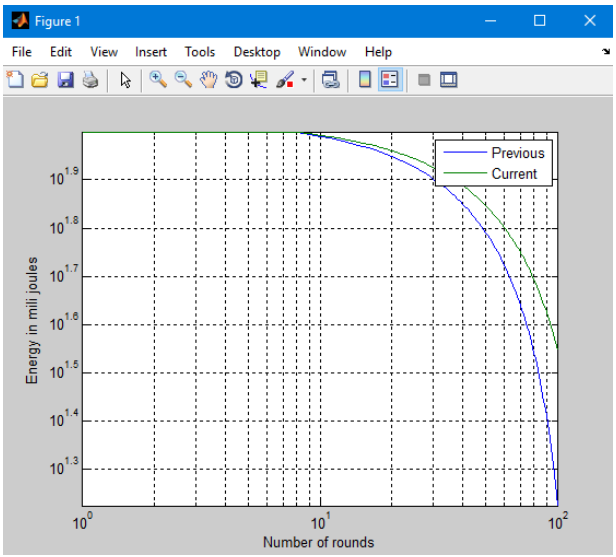


Fig: 3 Energy in mile joules versus Number of rounds

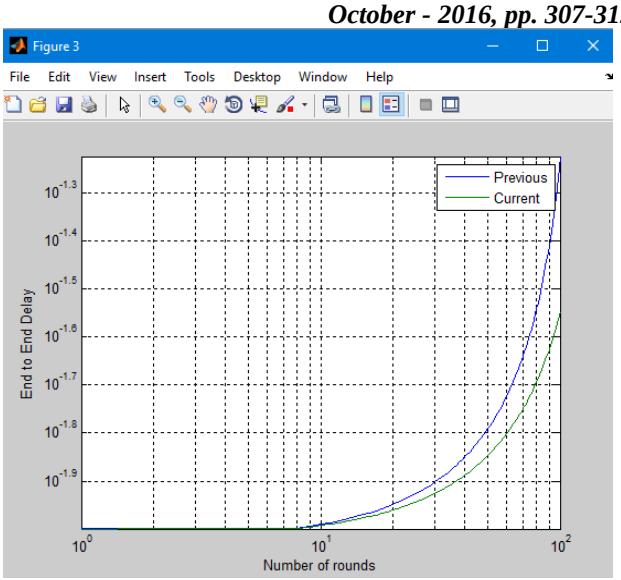


Fig: 4 End to End Delay versus Number of rounds

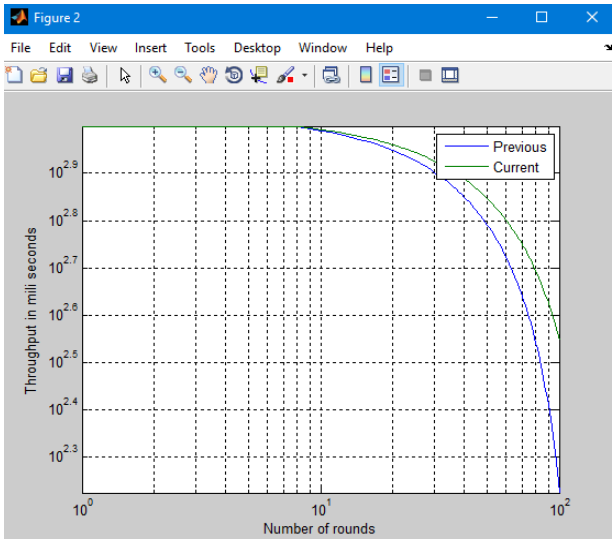


Fig: 5 Throughput in mile sec versus Number of rounds

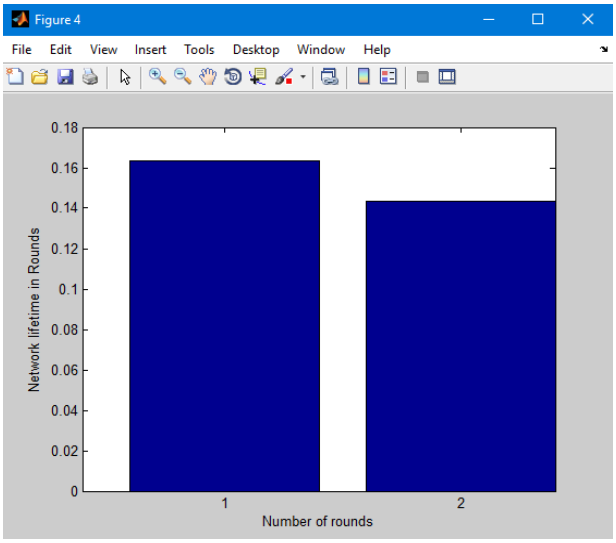


Fig. 6 Network lifetime in Rounds versus no. of rounds

## VI. CONCLUSION AND FUTURE WORK

In this paper we have studied the old grade trust scheme in order to detect the malicious attacker causing hello flood attacks in the network. We have modified the old Grade Trust scheme that was used in to detect the malicious black hole nodes in the network. In modified scheme we worked to analyse the impact of the Hello flooding attack on the network, to modify the Grade Trust Scheme to detect the flood attacker nodes in the network, to implement the modified scheme in MATLAB and to compare the performance of the network after applying the Grade Trust scheme and in the presence of the attackers. The results of the new modified scheme shows that the new scheme is more efficient then old scheme as it has less energy consumption, reduced end to end delay and maximum throughput .In the future work of the scheme we would work to make the grade trust scheme more efficient in which we will study the history of nodes and on the basis of their performance we could increase or decrease the trust value of the node in the network.

## REFERENCES

[1] Wang, D. and Wang, P., 2014. Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks. Ad Hoc Networks, 20, pp.1-15.

[2] Ferraz, L.H.G., Velloso, P.B. and Duarte, O.C.M., 2014. An accurate and precise malicious node exclusion mechanism for ad hoc networks. Ad hoc networks, 19, pp.142-155.

[3] Perkins, C., Belding-Royer, E. and Das, S., 2003. Ad hoc on-demand distance vector (AODV) routing (No. RFC 3561).

[4] Zhang, C., Zhu, X., Song, Y. and Fang, Y., 2010, March. A formal study of trust-based routing in wireless ad hoc networks. In INFOCOM, 2010 Proceedings IEEE (pp. 1-9). IEEE.

[5] Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A. and Nemoto, Y., 2007. Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method. IJ Network Security, 5(3), pp.338-346.

[6] Li, X., Lyu, M.R. and Liu, J., 2004, March. A trust model based routing protocol for secure ad hoc networks. In Aerospace Conference, 2004. Proceedings. 2004 IEEE (Vol. 2, pp. 1286-1295). IEEE.

 

[7] Al-Shurman, M., Yoo, S.M. and Park, S., 2004, April. Black hole attack in mobile ad hoc networks. In Proceedings of the 42nd annual Southeast regional conference (pp. 96-97). ACM.

[8] Raj, P.N. and Swadas, P.B., 2009. Dpraodv: A dyanamic learning system against blackhole attack in aodv based manet. arXiv preprint arXiv:0909.2371.

[9] Deng, H., Li, W. and Agrawal, D.P., 2002. Routing security in wireless ad hoc networks. IEEE Communications magazine, 40(10), pp.70-75.

[10] Pushpa, A.M., 2009, December. Trust based secure routing in AODV routing protocol. In Internet Multimedia Services Architecture and Applications (IMSAA), 2009 IEEE International Conference on (pp. 1-6). IEEE.

[11] Albers, P., Camp, O., Percher, J.M., Jouga, B., Me, L. and Puttini, R.S., 2002, April. Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches. In Wireless Information Systems (pp. 1-12).

[12] Cordasco, J. and Wetzel, S., 2008. Cryptographic versus trust-based methods for MANET routing security. Electronic Notes in Theoretical Computer Science, 197(2), pp.131-140.

[13] Marchang, N. and Datta, R., 2012. Light-weight trust-based routing protocol for mobile ad hoc networks. IET information security, 6(2), pp.77-83.

[14] Marti, S., Giuli, T.J., Lai, K. and Baker, M., 2000, August. Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the 6th annual international conference on Mobile computing and networking (pp. 255-265). ACM.

[15] Safa, H., Artail, H. and Tabet, D., 2010. A cluster-based trust-aware routing protocol for mobile ad hoc networks. Wireless Networks, 16(4), pp.969-984.

[16] Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. IEEE.

[17] J´unior, W. R. P., Figueiredo, T. H. de P., Wong, H. C., & Loureiro, A. A. F. (2004). Malicious node detection in wireless sensor networks. IEEE.

[18] Stetsko, A., Folkman, L., & Matyáš, V. (2010). Neighbor-based intrusion detection for wireless sensor networks. Proceedings of 2010 6th International Conference on Wireless and Mobile Communications (ICWMC) (pp. 420-425).

[19] Peng, B. C., & Liang, C. K. (2006). Prevention techniques for flooding attacks in Ad-Hoc networks. IEEE.

[20] Luis E. Palafox, J. Antonio Garcia-Macias,(2008) Security in Wireless Sensor Networks, IGI Global, Chapter 34.

[21] Waldir Ribeiro Pires Junior Thiago H. de Paula Figueiredo Hao Chi Wong Antonio A.F. Loureiro, "Malicious Node Detection in Wireless Sensor Networks," 18th International Parallel and Distributed Processing Symposium(IPDPS'04) Vol. 1, pp. 24, 2004

 