

# REINFORCEMENT SECURITY FOR MOBILE AD HOC NETWORKS WITH TRUST MANAGEMENT SCHEME

Adhithiya.E<sup>#1</sup>, Satheesh.R<sup>#2</sup>

#1 PG scholar, Arunai Engineering College, Tiruvannamalai, TamilNadu, India, 9042050846,  
eadhithiya19@gmail.com

#2 Faculty (EEE), Arunai Engineering College, Tiruvannamalai, TamilNadu, India, 9790413286,  
satheeshrped@gmail.com

## ABSTRACT

MANET (Mobile ad hoc network) is a collection of mobile nodes, which forms a temporary network, security is the major issues in this fields. Here trust management is indirect observation of node from neighbor nodes which is derived using dempster-shafer theory. In this paper cumulative sum (CUSUM) algorithm is used to enhance security in mobile ad hoc network, where CUSUM algorithm based on Location Interference Routing (LIR) which causes longer detection delays and a lower detection rate, so multi-class CUSUM algorithm is proposed. Results show that the proposed algorithm achieves a higher and more accurate rate of detection with ad-hoc on-demand distance vector (AODV) routing protocol with Network simulator 2 (NS2).

**Key terms:** Dempster-shafer theory, CUSUM, AODV.

**Corresponding Author:** [Adhithiya.E](mailto:Adhithiya.E)

## INTRODUCTION

Collection of independent nodes combined to form a network called MANET. Mobile ad hoc networks is an infrastruceless networking i.e. it communicate without any predefined infrastructure or centralized authority [1].The main countenance of are it a distributed operation and multi hop routing. For communication, members of node uses wireless interface which themselves sensible for operation and maintenance of the network.

Enhancing security in MANETs is a key issue in constrain field such as military environments [2]. All networking functions such as routing and packet forwarding, are performed by nodes themselves in a self-organizing manner. For these reasons, securing a mobile ad-hoc network is very challenging. The goals to evaluate if mobile ad-hoc network is secure or not are as follows[4]: 1) *Availability*: It means the node assets are accessible only to authorized user at appropriate times which refers to both data and service. 2) *Confidentiality*: Confidentiality means only the authorized user can access all the assets of each node in a network. It also protect against unauthorized reading of messages. 3) *Authentication*: Authentication naturally gives assurance that nodes in communication are authenticated and not imitators. 4) *Integrity*: Integrity means that assets can be reform only by authorized nodes or only in authorized way which avoid the corruption. 5) *Authorization*: This property assigns different access rights to different types of users. For example a network management can be performed by network administrator only. Mobile ad hoc network can be used for communication in military battlefield, business environment, commercial sector and etc...In this paper the algorithm is proposed to improve the security constrain field such as military environment as shown in figure 1.

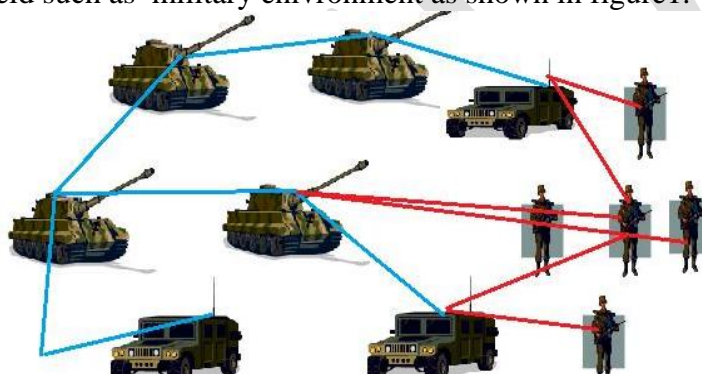


Figure 1: Application of MANET

Trust management is a unified approach which acts as a separate security services in network which is used to specify and interpret security policies and relationships. Trust management here done with direct and indirect observation of nodes [3]. In this paper, we propose Dempster-Shafer theory which an indirect observation to identify malicious users. CUSUM algorithm[4] with accurate detection, less computation and commonly used in anomaly detection suitable for MANET than any other algorithm. Cumulative sum is computed by comparing nodes with a predefined thresholds for detecting of attackers. AODV[5] is a reactive protocol in which each node does not require to maintain routes for destination and so secured transformation here we are using AODV.

## TRUST MANGEMNET WITH INDIRECT OBSERVATION

In this section we discuss about the trust value of the node is evaluated using indirect observation of neighbor node. Normally in direct observation, an observer will assessing trust value of this same node [10]. But in indirect observation neighbor's opinion will help in judgment of reliable of the observer node. Here collection of neighbor's opinion is major part for determining whether a node is authorized or not, the trust value of indirect observation is derived using Dempster-Shafer theory. To derive this theory at first we define a user's behavior value which is a binary value to indicate whether node is suspicious or not. When the node rating is suspicious, then the behavior value of  $u_j$  for  $I_i$  denoted by  $Beh_{u_j}(i)$  is set to 0. otherwise  $Beh_{u_j}(i)$  is set to 1. Combined behavior value of  $u_j$ 's on  $r+s$  items as

$$Beh_{u_j}^{com} = \frac{r}{r+s+2}, \text{ and the behavior uncertainty for this same } r+s \text{ items as}$$

$$Beh_{u_j}^{uncer} = \frac{2}{r+s+2}.$$

Consider that a user  $u_j$  has rated N items  $(I_1, I_2, \dots, I_i, \dots, I_N)$  in total, except item  $I_i, u_j$  has behavior value as 0 on s items.  $I_i$  is calculated as on trust rating provided by user  $u_j$  on item  $I_i$  then  $T_{ui}(i)$ ,

$$T_{u_j}(i) = Beh_{u_j}^{com} * (1 - Beh_{u_j}^{uncer}) + Beh_{u_j} * Beh_{u_j}^{uncer}$$

$$= \frac{r}{r+s+2} * \frac{r}{r+s+2} + Beh_{u_j}(i) * \frac{2}{r+s+2} \quad (1)$$

Thus the malicious users is detected using low trust values on items  $I_i$ . only yield low trust values are removed instead of removing all the ratings provided by the malicious node. Here  $u_j$  is rating to  $I_i$  be removed which is marked as malicious user. Hence trust threshold value, changes according to different scenarios.

### CUSUM ALGORITHM

In Mobile ad hoc networks for anomaly detection we propose cumulative sum (CUSUM) algorithm which has less computation, exact detection and non-parametric features. Normally it is developed for independent and distributed variables  $\{x_j\}$  since CUSUM is a hypothesis testing. Let the ratio test between observed and the original assumption is:

$$C_{n,v} = \frac{\prod_{i=1}^u \phi(x_i) \prod_{i=u+1}^n \phi(x_i - \delta)}{\prod_{i=1}^n \phi(x_i)}$$

$$= \exp \left\{ \delta \sum_{i=n+1}^n \left[ x_i - \frac{\delta}{2} \right] \right\} \quad (2)$$

where  $\prod_{i=1}^n \phi(x_i) = 1, \sum_{i=u+1}^n x_i = 0.$

Logarithm value of (2) is taken to determine offset and original assumption will be:

$$\Lambda_n = \max \left\{ \delta \sum_{i=u+1}^n \left[ x_i - \frac{\delta}{2} \right] \right\} \quad (3)$$

If an upward shift is detected then the original assumption is equal to the following test:

$$Z_n = \max_{1 \leq u < n} \left\{ \sum_{i=u+1}^n \left[ x_i - \frac{\delta}{2} \right] \right\} \quad (4)$$

The above (4) represents the CUSUM values with amplitude percentage parameter and the alarm threshold h and also length of time interval over which traffic are measured in normal conditions when the network is in under attack.

### Multi-Class CUSUM Algorithm

In this proposed work multi-class cumulative sum algorithm is used with small parameters  $(k, \theta)$  which prevent attacks, traffic control. The main reason for selecting multi class cumulative is reduces the single threshold which leads to longer delay for an alarm. This cannot be possible in CUSUM algorithm even it process with light weight accurate detection. Let  $X_{i,1}, X_{i,2}, \dots, X_{i,h}$  be an independent and same distributed variables for terms  $N(0,1)$ . for  $N(\delta,1)$  the variables will be  $X_{i,h+1}, X_{i,h+2}, \dots$  where h is threshold. The mean flow of sequence is:

$$M_i = \frac{1}{n} \sum_{j=0}^n x_{i,j}, i = 1, 2, \dots, m \quad (5)$$

For traffic sequence  $i$ , where  $\theta$  is thresholds of different flow sequences, during the time period  $h-1$  when anomaly is not detected then necessary conditions of abnormality is:

$$\begin{cases} Y_{i,n} \leq \theta_i \\ Y_{i,h} > \theta_i \end{cases} \quad i = 1, 2, \dots, m; n = 1, 2, \dots, h-1, \quad Y_{i,n} = (Y_{i,n-1} + Z_{i,n})^+, Y_{i,0} = 0.$$

$X^+$  is defined as,

$$X^+ = \begin{cases} x, & x > 0 \\ 0, & x \leq 0 \end{cases}$$

### EXPERIMENTAL RESULT AND ANALYSIS

#### A. Parameter Configuration:

To make MANET a comparative analysis for performance related models we use NS2 (Network Simulator 2) platform along with routing protocol ad hoc on demand distance vector (AODV). Since AODV as specialized characteristics such as loop free routing, figure 2 and 3 shows detecting attackers and eliminating it. The multi-class CUSUM algorithm evaluated through the features of traffic, the CUSUM values with the true positive rate and false positive rate of sensor node. Below table represents the parameter configuration using this simulator.

Table1- Simulation parameter

Parameter	Value
Network size (m <sup>2</sup> )	1000 x 1000
Number of nodes	50
Traffic type	CBR traffic flow
Network protocol	IPv4
MAC protocol	IEEE 802.11b
Routing protocol	AODV
Packet size	512 bytes
Simulation time	300s

1) Packet delivery ratio: It is ratio of number of data packets delivered successfully from source to destination node at regular intervals which also illustrates the intensity of delivered data to destination. Figure 4 shows the PDR of number packet received at destination, whenever the results getting greater values of PDR means protocol done a better performance with different traffic models. Since here we are using AODV protocol its shows greater value which as better performance.

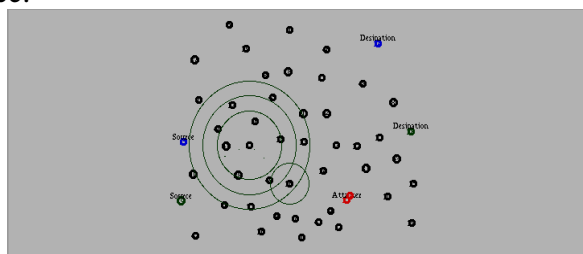


Figure 2: detecting attackers

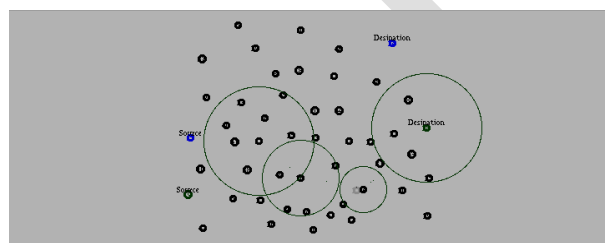


Figure 3: Annihilating attackers

2) Average end-to-end delay: It is the time taken by a packet to arrive destination after leaving the source. Commonly average delay is calculated by adding individual packets delay and dividing it by number of packets transmitted. Figure 5 shows the average end- to-end delay. In AODV time taken for RQ-PEER is more than RE-PEER this is because link breakage is minimized in AODV.

3) Throughput: Throughput is the rate of successful delivery of data from source to destination nodes. It calculated as bits per seconds or data packets per seconds. Figure 6 shows the throughput of the network it is the sum of all the nodes in the networks.

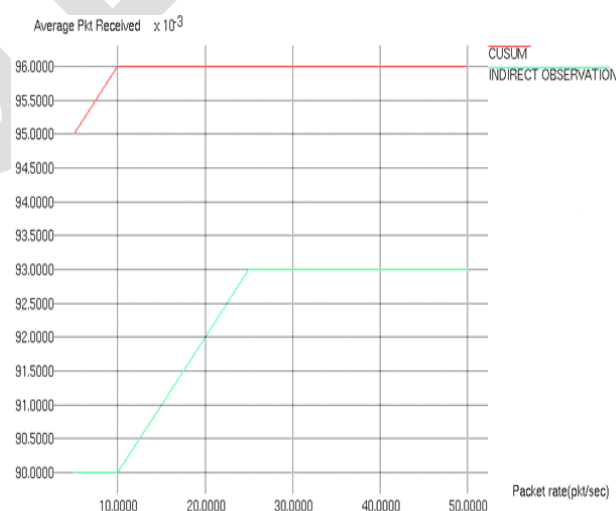


Figure 4: Packet delivery ratio

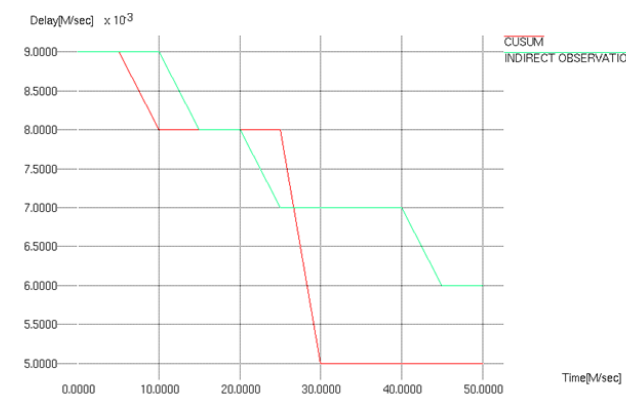


Figure5: Average end-to-end delay

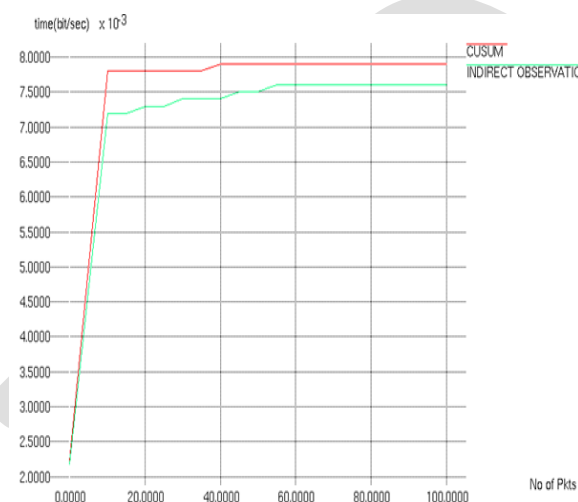


Figure6: Throughput ratio

## CONCLUSION

In the paper, enhancing of security in Mobile ad-hoc networks (MANET) is simulated using NS2 based on multi-CUSUM algorithm which is change point detection it is used for anomaly detection. Using this proposed algorithm, performance is improved and also diminishes the average end-to-end delay. For trust management scheme here we used indirect observation which is derived using dempster-shafer theory. It is scenario based on behavior uncertainty values and parameters. Simulation results show that the Ad-hoc on-demand distance vector (AODV) routing protocol packet delivery ratio values are increased greatly and by less energy 'consuming AODV reduces average end-to-end delay in the networks. Throughput values also improved i.e. number of packets delivered to destination is increased using this proposed protocol.

## REFERENCE

[1] Burmester de Medeiros, On the security of route discovery in MANETs ,*IEEE Transaction on mobile computing*, volume:8,issues:9,pp.1180-1188,jan 2009.

[2] Saervita Semaplay, Rajni Sobti and Venu Mangats, Review: trust management in MANETs, *International journal of Applied Engineering research*, volume: 7, pp.1-4issues:11, Sep 2012.

- [3] Zhexiong Wei, Helen Tang, F. Richard Yu, Maoyu Wang, and Peter Mason, Security Enhancements for Mobile Ad Hoc Networks with Trust Management Using Uncertain Reasoning, *IEEE Transactions on Vehicular Technology*, volume: PP, issue: 99, pp.1-12, April 2014.
- [4] Tongguang Zhang, Cumulative sum algorithm for detecting SYN flooding attacks, *IEEE Transaction on wireless communication*, volume: 3, no: 3, March 2014.
- [5] Rochi, Dana, Ziyaae, A new source routing mechanism in mobile ad-hoc networks, *International conference on Advanced communication technology (ICACT)*, pp. 948-952, Feb 2011.
- [6] Aravindh, Vinoth, Vijayan, A trust based approach for detection and isolation of malicious nodes in MANET, *International journal of Engineering and technology (IJET)* volume: 5, pp.193-199, March 2013.
- [7] Dhanalakshmi, Kannapiran, Divya, Enhancing manet security using hybrid techniques in key generation mechanism, *International conference on Electronics and communication system (ICECS)*, volume: 6, pp.1-5, Feb 2014.
- [8] Razuqi, Bousherhri, Gaballah, alsaleh, Extensive simulation performance analysis for DSDV, DSR and AODV MANET routing protocols, *International conference on advanced information networking and application workshops (WAINA)*, pp.335-342, March 2013.
- [9] BoYang, Yammamoto, Tanaka, Dempster-shafer evidence theory based trust management strategy against cooperative black hole attacks and gray hole attacks in MANETs, *International conference on Advanced communication technology (ICACT)*, pp.223-232, feb 2014.
- [10] Chen, Venkataramanan, Dempster-shafer theory for intrusion detection in ad hoc networks, *IEEE Internet computing*, volume: 9, issues: 6 pp.35-41, Nov 2005.
- [11] Yuhong Liu, Yan Sun, Siyuan Liu, Kot, Securing online reputation systems through trust modeling and temporal analysis, *IEEE transaction on Information Forensics and security*, volume: 8, issue: 6, pp.936-948, june 2013.
- [12] Vasilios, Fotini Papagalou, Application of anomaly detection algorithms for SYN flooding attacks, *IEEE international conference on network* volume 29, issue 9, pp.1433-1442, 2014.
- [13] Callegari, Giordano, pangano, pepe, Combining wavelet analysis and CUSUM algorithm for network detection, *IEEE conference on communication and information system security (ICC)* pp.1091-1095, June 2012.
- [14] Vaswani, The modified CUSUM algorithm for slow and drastic change detection in general HMMs with unknown change parameters, *IEEE international conference on ICASSP* volume 4 pp: 701-704, march 2005.