TFT Technique with Adaptive Thresholding for Selfish Attack Prevention in MANET

Ankita Verma
PG Research Scholar
Department Of CSE,
RITS, Bhopal (M.P)

Ashish Khare
Assistant Professor
Department Of CSE,
RITS, Bhopal (M.P)

ABSTRACT
This paper presents an Adaptive Trusted Fault Tolerance (TFT) scheme with Data Recovery for the prevention of selfish attack in MANET it also prevents the packets drop caused by the buffer overflow of the node. In the proposed technique an adaptive variations in trust certification waiting time is proposed instead of simple TFT schemes, which helps reduces the false identification of nodes during heavy load conditions it also reduces the identification delay during the light load conditions. The proposed model is simulated using OPNET network simulator and the simulation results shows that the proposed algorithm performs better than simple Trusted Fault Tolerance (TFT) scheme.

Keywords
MANET, Trusted Fault Tolerance (TFT), Selfish Attack.

1. INTRODUCTION
Mobile Ad-Hoc Network (MANET) is decentralized wireless system where the node connects dynamically without central administration. MANETs consist of mobile nodes that are free in moving in and out in the network, here nodes are defined as systems or devices like personal computer, Laptop, mobile phone or any other electronic system which is player and personal computer that are participating in the network and able to move.

Since the nodes in MANET not only communicates itself but also helps others by forwarding there packets hence these nodes can act as host or router or both at the same time.

Because there is centralized controlling and also no control over movement of nodes they can form random topologies depending on their connectivity establishment with each other in the network. The ability to configure themselves and depends upon the routing protocol they adopt. Routing protocols is one of the challenging and interesting research areas. Many routing protocols have been developed for MANETS, i.e. AODV, OLSR, DSR etc. Because of no centralize control the network it very often suffer from security attacks & that is why the security in Mobile Ad-Hoc Network is considered as the most important concern for the proper functionality of network. Till now many types of attack are known in MANET but in this paper we considered only

selfish attack. Selfish Nodes can be described as a node which does not forward other's packets, thus maximizing their benefit at the expense of all others. They are assumed to always behave rationally, so they cheat only if it gives them an advantage.

2. LITERATURE REVIEW

This section presents some of the useful articles related to our work. A mathematical model presented by Md. Amir Khusru Akhtar & G. Sahoo [2] in they presented the mathematical model to detect selfish nodes using the probability density function. Their proposed model works with existing routing protocol and the nodes that are suspected of having the selfishness are given a Selfishness test they also formulates this problem with the help of prior probability and continuous Bayes theorem & verified the mathematical by experimentation which shows acceptable accuracy. Another mobile agent based approach is presented by [3] Debdutta Barman Roy and Rituparna Chaki their approach utilizes the mobile agents and because mobile agents can move from one node to another they works as a distributed system which reduces the data transferring requirements to any particular node & reduces network bandwidth consumption and the results shows decreases in the computation overhead in each node in the network. Frank Kargl, Andreas Klenk, Stefan Schlott, and Michael Weber [4] presented a comparative analysis of different techniques used for selfish node detection and also proposed new detection mechanisms called activity-based overhearing, iterative probing, and unambiguous probing. They also point out the limitation of their technique that is all the thresholds need to be set manually in order to get good detection results. So in the future we will try to find ways how these values can be set and adjusted automatically during operation. Martin Schütte [5] outlines important attacks and summarizes popular approaches to design secure MANET protocols in order to detect selfish and malicious nodes and to enforce cooperation. This work contains some very useful methods and their explanations. A cross layer approach for selfish node detection in MANET is proposed by Prof. Rekha Patil, Shilpa Kallimath [8]. Fuzzy Based Security Model for compromised & selfish node detection is presented by M. B. Mukesh Krishnan & P. Sheik Abdul Khader [10] they presented a fuzzy based security model to detect the compromised and selfish nodes. Both of the nodes are detected by estimating the trust level of the nodes using the process named trust verification, trust hold setting and fuzzy based attack analysis process. They also validated the model by simulating it. Chandrasekaran S. & Shanmugam

Udhayakumar presented a Trusted Fault Tolerant Model of MANET with Data Recovery [1] their work shows a simple and effective method for selfish attack problems in our proposed system we also utilized it with dynamic modification of threshold time.

3. Selfish Node Characteristics

These nodes aim to get the greatest benefits from the networks while trying to preserve their own resources, e.g. battery life or bandwidth. Selfish nodes attempt to maintain communications with the nodes it wants to send data packets to but may refuse to cooperate when it receives routing or data packets that it has no interest in. Therefore, it may either drop data packets or refuse to retransmit routing packets when it has some contradictory goals. [8].

4. Selfish Node Problem

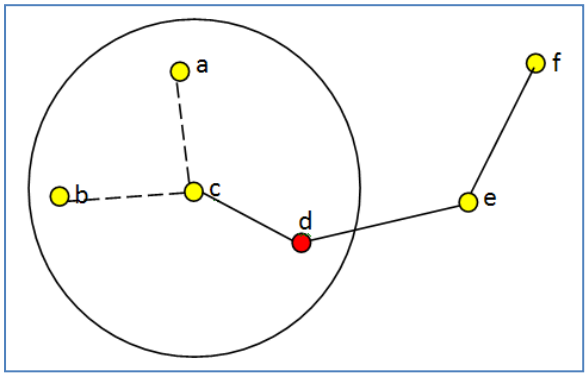

Figure 1: Selfish Node Problem Demonstration

Taking the reference of figure 1 let we assume that node c wants to send a packet to f for this purpose the node c firstly starts the route discovery and broadcast the route request since only d can complete the route for c to f but in this case d is a selfish node hence it will behaves like a failed node (in some cases It is possible that d can forward control packets but it will not forward the data packet). Hence d will discard all data to be forwarded through it which result a failed communication. Since the node is selfish it can still communicate with other nodes when it is required by itself.

5. Proposed Algorithm

5.1 Route Selection

In the proposed method during the route selection each route is ranked by the trust rating of the nodes forming that route. The route with node which having highest minimum trust rating is selected.

Table1: Route Table with Nodes and their Trust ratings (in brackets)

Route A	A(3)	B(4)	C(1)	D(4)
Route B	A(2)	B(3)	E(2)	D(4)

For example in above table Route B will be selected it having the highest minimum trust value of 2 than the Route A which have the minimum value of 1.

5.2 Trust Rating

The trust rating of the node in the system is formed by the subtraction of negative votes from positive votes given by surrounding nodes. The positive vote is a packet which is generated by surrounding nodes when the node forwards the received packet within specific time called threshold time otherwise they generates the negative vote.

5.3 Normal Working

As the node transmits a packet it waits for the threshold duration to get the acknowledgement from the node to which the packet was sent. If the required acknowledgement is not received within the threshold duration alternate nodes are selected & a recovery manager gets activated which loads the packets from the node buffer onto a recovery buffer and flushes the contents of the node buffer for security purposes [1].

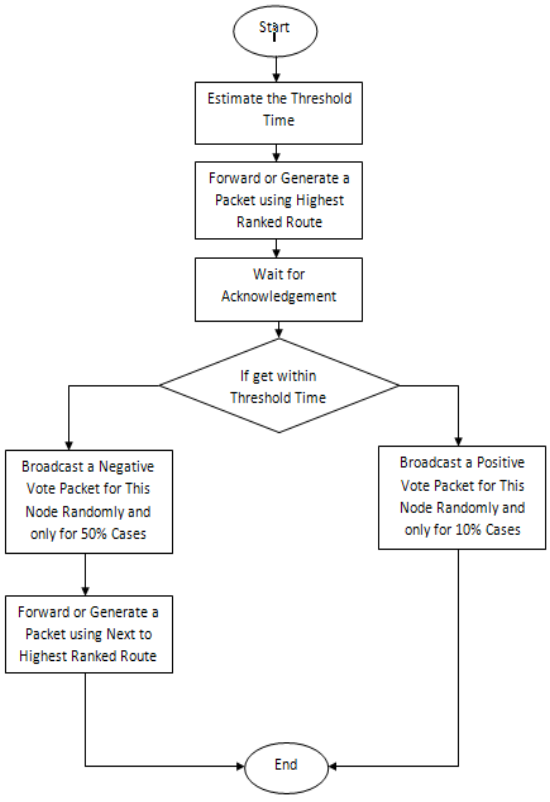

Figure 2: Simplified Flowchart of the Proposed Algorithm.

6. Simulation Results:

The proposed algorithm is simulated using OPNET network simulator with following configurations shown in Table 2:-

Network Area	1kmX1km
Node RF transmission Power	10 mW
Routing Protocol	DSR
Number of Nodes	18
Mobility	Hexagonal Path
Packet Generation	exponential (1024)
Packet Inter-arrival Time	exponential (1)
Simulation Time	20 minutes

Following Colors are used in graphs shown in Table 3:-

Red:	the network without Attack
Blue:	when attack is applied on the network
Green:	Securing the network with fixed Threshold Time.
Light Blue:	Securing the network with adaptive threshold time.

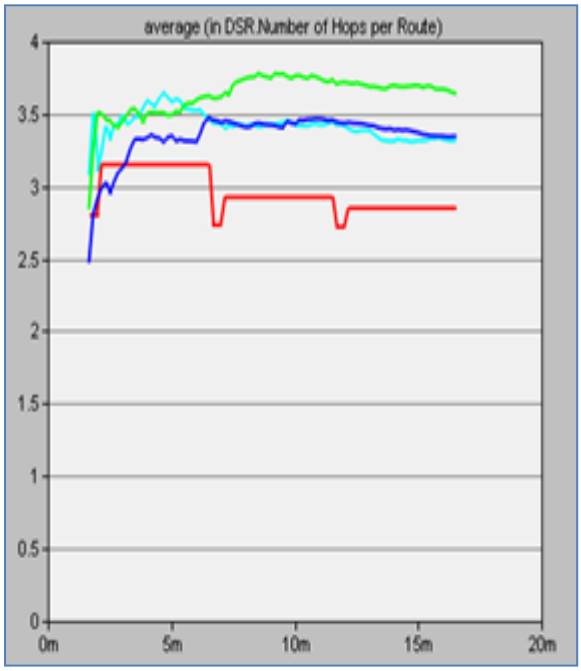

Figure 3: this figure shows that how the number of hops per route varies with different conditions during normal case this remains lowest and attack increases it to maximum and when the solution is applied it falls back this shows that the proposed technique works perfectly.

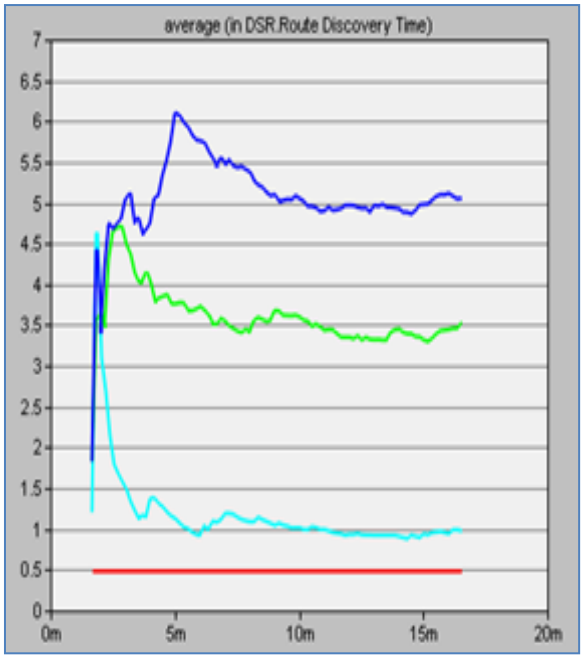

Figure 4: the route discovery time increases during attack as node isolation could possible and when we apply the proposed techniques it settle to almost its normal position.

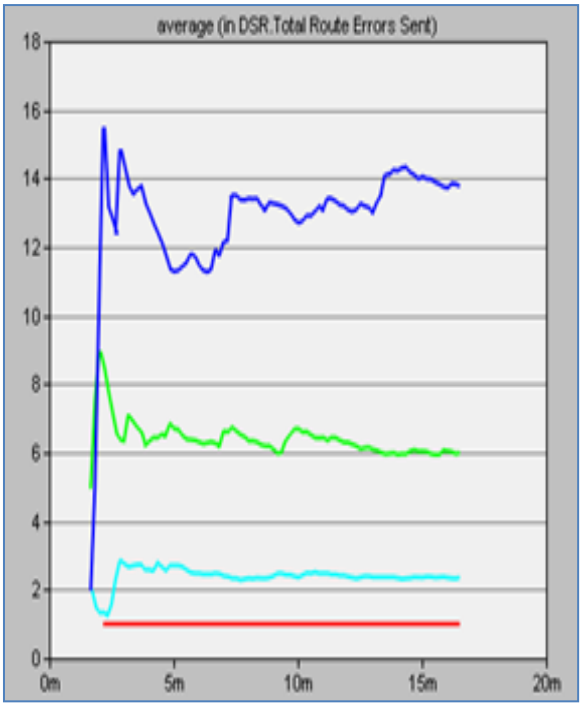

Figure 5: This graph presents the variations in total route errors and this also shows that the adaptive thresholding performs best.

7. Conclusion

The simulated results shows that the adaptive thresholding is better solution than the fixed because the packet forwarding time may vary with traffic load which can cause false detection with fixed thresholding. Present simulation also

shows that the adaptive thresholding enhance the performance (QoS) of the network.

8. References

[1] Chandrasekaran S & Shanmugam Udhayakumar "Trusted Fault Tolerant Model of MANET with Data Recovery", 2011 Fourth International Conference on Intelligent Networks and Intelligent Systems.

[2] Md. Amir Khusru Akhtar & G. Sahoo "Mathematical Model for the Detection of Selfish Nodes in MANETs", International Journal of Computer Science and Informatics (IJCSI) ISSN (PRINT): 2231 –5292, Volume-1, Issue-3.

[3] Debdutta Barman Roy and Rituparna Chaki "MADSN: Mobile Agent Based Detection of Selfish Node in MANET", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 4, August 2011.

[4] Frank Kargl, Andreas Klenk, Stefan Schlott, and Michael Weber, "Advanced Detection of Selfish or Malicious Nodes in Ad hoc Networks".

[5] Martin Schütte "Detecting Selfish and Malicious Nodes in MANETs", SEMINAR: SICHERHEIT IN SELBSTORGANISIERENDEN NETZEN, HPI/UNIVERSITÄT POTSDAM, SOMMERSEMESTER 2006.

[6] Niyati Shah, Sharada Valiveti "Intrusion Detection Systems for the Availability Attacks in Ad-Hoc Networks" International Journal of Electronics and Computer Science Engineering.

[7] YOGESH CHABA, YUDHVIR SINGH, PRABHA RANI "Comparison of Various Passive Distributed Denial of Service Attack in Mobile Adhoc Networks", RECENT ADVANCES in ELECTRONICS, HARDWARE, WIRELESS and OPTICAL COMMUNICATIONS.

[8] Prof. Rekha Patil, Shilpa Kallimath "Cross Layer Approach for Selfish Node Detection in MANET" International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE) Volume 1, Issue 3, September 2012.

[9] Amit Saxena, J.L Rana "Analysis of Selfish and Malicious Nodes on DSR Based Ocean Protocol in MANET" TECHNIA International Journal of Computing Science and Communication Technologies, VOL. 3, NO. 1, July 2010. (ISSN 0974-3375).

[10] M. B. Mukesh Krishnan, P. Sheik Abdul Khader "Fuzzy Based Security Model to Detect Compromised and Selfish Nodes to Mobile AD HOC Network" European Journal of Scientific Research ISSN 1450-216X Vol. 86 No 4 September, 2012, pp.520-524.

[11] Naveen Kumar Gupta, Ashish Kumar Sharma, Abhishek Gupta "Selfish Behaviour Prevention and Detection in Mobile Ad-Hoc Network Using Intrusion Prevention System (IPS)".

[12] T.V.P.Sundararajan, Dr.A.Shanmugam "Modeling the Behavior of Selfish Forwarding Nodes to Stimulate Cooperation in MANET" International Journal of Network Security & Its Applications (IJNSA), Volume 2, Number 2, April 2010.