A SURVEY OF FALSE ALARM ALGORITHMIN PRESENCE OF MALICIOUS NODE FOR MOBILE AD-HOC NETWORKS

Lalita Nayak [1], Rashmi Priyanka[2] , Palak Keshwani[3]

[1][2][3]Asst. Professor , KITE Raipur

E-mail : - lalitanayak2010@gmail.com, rashmi.priya2@gmail.com, palakeshwani@gmail.com

ABSTRACT

As the network size and application level of mobile ad hoc networks increases, the numbers of security parameters needed by such algorithms become more and more efficient. Mobile ad hoc network has dynamic architecture which thus provides rights to malicious node to modify or delete data or reroute the data transmission path. If the centralize administration is not present then malicious node may also leave the network architecture. False alarm algorithm plays a vital role to detecting malicious nodes present in the mobile ad hoc network. False alarm algorithm produces an alarm when it detects the malicious node and notifies other neighbor nodes and network admin. In this paper we survey the past and present year on False alarm algorithm, which observe and analyze these algorithms.

Keywords: *Manet, Fpr, Aodv*

1. Introduction

In current situation, mobile ad hoc networks have been get more concern due to their properties of highly dynamic, multi-hop, lack of central structure, and infrastructure-less. Especially, mobile ad hoc networks are widely used in specialized areas or relief environment such as emergency operations, battlefields, disaster recovery in such situations like flood or earthquake, and suitable for wired andwireless networks etc. Mobile ad hoc networks have wide applications;since it has the various numbers of services provided by mobile ad hoc networks are rapidly increasing. It is major task to identify malicious nodes becomes complex challenge of mobile ad hoc network. Since mobile ad hoc network has dynamic infrastructure, in which malicious node has malicious activities like modifying data, deletion of data, rerouting. Mobile ad hoc network is suffering from lacking of centralized administration which causes malicious nodes to creating loopholes thus reflecting innocent nodes to leaving network. False alarm algorithms plays vital role to detecting malicious node in the mobile ad hoc network. Most of the intrusion management uses False alarm algorithm for good utilization of packets in the MANET and usability of MANETs. There have been various intensive research efforts and extensive applications in the domain of False alarm algorithms of most Ad hoc networks.

The Basic Idea of False Alarm Algorithm

A false alarm algorithm is an alert alarm. If the malicious node present in the network and causes unwanted variation where they are not needed in the MANET then false alarm algorithm generate erroneous report and notify to other neighbor nodes.False alarms may raise when the nodes in network plays as malicious or selfish.

Various Classification of False Alarm Algorithm in Mobile Ad Hoc Networks:

1) Based onInfrastructure network: Mobile ad hoc networks usually been based on the cellular methodology and depend on good infrastructure support, in which mobile nodes communicate with each access points such as base stations connected to the fixed network infrastructure where false alarm will be activated from base station if any falsify node detected.

2) Based on Infrastructure less network: In infrastructure less technique there is no central administration involvement is done for the entire network. The MANETis infrastructure less in a way that commonly known as a mobile ad hoc network (MANET). A mobile ad hoc network is a collection of wireless nodes that can dynamically changes their position to form a network to exchange information without using any fixed stationary network architecture. Here false alarm algorithm used to identify the malicious node occurs in the network.

2. Related Work

In this section we provide extensive description of the existing false alarm protocols, which are grouped according to the taxonomy, defines in the introduction of this paper.

2.1 An Acknowledgment-based Approach for the Detection of Routing Misbehavior in MANETs

The authors [1] suggest a routing protocol for mobile ad hoc network which is based on theory that the nodes in network are collaborative with neighbor nodes. Since mobile ad hoc network is lacking of central administration and has open structure node may misbehave in network.Such routing misbehavior causes malicious nodes that will involve in the route creating and maintenance activities but deprive to forward data packets. In this paper, they propose the 2_ACK methodology that provides process as an add-on method for routing methodology which is used to identify routing misbehavior and to minify their unfavorable effect.The motive of the 2_ACK method is to transmit two-hop ack packets in the opposite side of the routing path. In 2_ACK scheme acknowledged received data packets is used to minimize routing overhead.

2.2 Technique to handle mischieveness in MANETs

In this paper [2], author said some nodes may selfishly behave only to coordinate randomly, or not at all, with other neighbor nodes in mobile ad hoc network. These malicious nodes could then minimize the overall network performance in the network which thus increase delay in data query. So many researchers have worked on this malicious node problem, and proposed various methodologies to identify these Mischiefs nodes. In this paper authors gives a survey on different techniques used to identify mischiefs nodes in Mobile ad hoc networks. It also gives information on data packet replication in a network, and certain techniques to handle malicious nodes. Authors suggest a collaborative watchdog along with method combined credit risk which thus increases network performance by identifying malicious nodes within short time period.

2.3 Detecting Selfish Nodes in MANETs

In this paper[3], every node plays two role first one is as a router and second one is as end-system and therefore each node in network is permitted tomove freely in any direction which makes routing path very difficult in network. Most of the routing algorithms used in mobile ad hoc network such as AODV and DSR which assume thatevery node will send every data packet it receive. In this methodology Source node will forward data packets to the destination node with the help of the

intermediate neighbor'snodes. However, misbehavior of the selfish nodes is a common phenomenon in MANET. These nodes usethe network and its services and do not provide any services to intermediate nodes in order to save energy such asbattery, CPU Power and band-width for relaying data from other nodes and reserve for themselves. These selfish nodeswill degrade the performances of wireless ad hoc networks. However, we can identify the selfish nodes by modifying theoriginal AODV and DSR routing algorithms. In this thesis, we proposed a time based scheme for identifying selfish nodes.

2.4 Derivative threshold actuation for single phase wormhole detection with reduction false alarm rate

In this paper[4], Data transmission in mobile Ad hoc networks is truly via multi-hop techniques. Owing to the distributed characteristics and bounded resource of nodes, MANET is having high risk to wormhole attacks i.e. wormhole attacks create severe problem to every Ad hoc routing protocol. Thus, so as to discover wormholes, totally diverse methods are in use. Our aim in this paper is to deduce the traffic threshold level by derivational approach for identifying wormholes in a very singlephase in relay network having dissimilar characteristics. In all those methods fixation of threshold is merely by trial & error methodology or by random manner. Conjointly wormhole detection is in twin part by putting the nodes that is higher than the edge in a suspicious set, however predicting the node as a wormhole by using some other algorithms.

2.5 Identifying false alarm in MANET in presence ofcongestion control

Since, the mobility is high, the nodes may move randomly and fast, which lead to network Partitioning. Most of the user sat different places assume that mobile nodes co-operate fully in terms of sharing their memory space. But the alarm will also be initiated because of network disconnections too but it seems and treated as overall selfishness alarm, it will affect the overall performance of the network. We have explored the impression of selfish nodes in a MANET from the perspective of replica allocation and developed selfish node detection algorithm that considers the partial selfish node and fully selfish node as selfish replica allocation. The behavior of these selfish nodes leads to decrease in over all data accessibility of the network. The replica will be allocated using specific SCF tree concept. To improve the data accessibility, we have proposed several data replication techniques. In this paper[5], the mobile nodes will have the characteristics of mobility and constraints in resources in mobile adhoc network. Detection of attacker node in the network and should be informed to all others in the network.

There is a source constraints lead to a big problem as decrease in performance and the network partitioning leads to poor data accessibility. But some nodes may decide as not to co-operate with others or partially co-operate with other nodes. An alarm will be raised based on the selfish behavior of overall nodes called overall selfishness alarm. The concept of this paper deals with detection of false alarm as differentiated from overall selfishness alarm and to inform the other nodes at route as exactly where the disconnections occur to select the next best alternative path and also to increase the performance with increased congestion control.

2.6 Identification of False Alarm in Handling of malicious Nodes in Mobile Ad Hoc Networks

Mobile ad networks do not have any existing infrastructure and they do not have any centralized administrator. In MANET each node acts as router. These nodes use the network and its services but they do not cooperate with other nodes. Several data replication techniques have been proposed to minimize performance degradation. These kind of selfishnodes do not consume any energy such as CPU power, battery and bandwidth for retransmitting the data of other nodes. They will

preserve the resources for their own use. So the MANET is self-creating, self-organizing and self-administrative wireless network. In this paper, [6] a mobile Ad Hoc network is a collection of mobile nodes. Most of them assume that all mobile nodes collaborate fully in terms of sharing their memory space. In practice some of the nodes may act as the selfish nodes. In reality, however, some nodes may selfishly decide only to cooperate partially, or not at all, with other nodes. These selfish nodes could then reduce the overall data accessibility in the network.

2.7 Selfish Node Detection Algorithm in Cluster Based MANET

In our proposal the MANET area has been split into a number of size clusters having cluster head and storage capability according to connectivity degree, RSS (relative signal strength) as per the cluster formation algorithm given. The idea behind clustering is to group the network nodes into a number of overlapping clusters. In this paper[7], Mobile Ad hoc network are collection of mobile nodes that can dynamically form temporary networks, it is necessary to bring the smart technologies in the Ad hoc network environment. In this cluster architecture we try to find false node inside clusters of MANET using a modified algorithm and try to removethem.In the clusters of mobile ad hoc network The resource constraints creates to a big problem as decrease in performance and the network partitioning leads to poor data accessibility due to false and selfish node. Huge amount of time and resources are wasted while travelling due to traffic congestion.

2.8 A Collaborative Intrusion Detection methodologiesfor Ad Hoc Network

In this paper[8], MANETs are highly vulnerable to attacks due to the open medium, dynamically changing network topology, cooperative algorithms, lack of centralized monitoring and management point, and lack of a clear line of defense So we report our progress in developing intrusion detection (ID) capabilities for MANET. Compared with the scheme where each node is its own ID agent, this scheme is much more efficient while maintaining the same level of effectiveness. For several well-known attacks, we can apply a simple rule to identify the attack type when an anomaly is reported. In some cases, these rules can also help identify the attackers. We address the run-time resource constraint problem using a cluster-based detection scheme where periodically a node is elected as the ID agent for a cluster. Building on our prior work on anomaly detection, we investigate how to improve the anomaly detection approach to provide more details on attack types and sources.

2.9 Dynamic Intrusion Detection System for MANET Using CPDOD Algorithm

Many of the intrusion detectiontechniques created on wired networks cannot be directly applied to MANET due to special characteristics of the networks. A series of experimental results demonstrate that the proposed method can effectively detect anomalies with low false positive rate, high detection rate and achieve higher detection accuracy. In this paper[9], Mobile Ad hoc networks are susceptible to several types of attacks due to their open medium, lack of Centralized monitoring and management point, dynamic topology and other features. However, all such intrusion detection techniques suffer from performance penalties and high false alarm rates. In this paper, we propose novel intrusion detection techniques by combining two anomaly techniques Conformal Predictor k nearest neighbor and Distance based Outlier Detection (CPDOD) algorithm.

2.10 Discarding Selfishness to enhance Replica Allocation over MANET's

These nodes could be detected and excluded from the cooperative portion of the network, as they only consume resources but don't contribute to the infrastructure. Some mobile nodes decided not to cooperate with other mobile nodes and simply aim to save its resources to the maximum while using the network to forward its own packets, these types of mobile nodes are called "Selfish Nodes" this misleading is very common in ad hoc network because of its configuration setup. In this paper [10], Mobile ad hoc networks are formed dynamically due to autonomous system of mobile nodes that are connected through wireless links without using an existing infrastructure or centralized administration. We have explored the impression of selfish nodes in a MANET from the perspective of replica allocation and developed selfish node detection algorithm that considers the partial selfish node and fully selfish node as selfish replica allocation. In this paper, a new mechanism that minimizes the problem of selfish nodes with the help of Credit risk and Brain trapping function Model. In existing methods, there are no steps to handle false alarms and efficient detection of selfish nodes. Including Degree of selfishness in allocating replicas will considerably reduce communication cost and produce high data accessibility.

3. Conclusion

The result after analysis has concluded and suggestion of mine is analyzing selfish node by using FAREP protocol is best when compared to above studied performance metrics. In this research paper, an effort has been made to concentrate on the comparative study and performance analysis of various False alarm methods to find selfish node in MANET on the basis of above mentioned performance metrics.

4. References

[1]. **Liu, Kejun, et al.** "An acknowledgment-based approach for the detection of routing misbehavior in MANETs." Mobile Computing, IEEE Transactions on 6.5 (2007): 536-550.

[2]. **Gayathry S S, RN Gaur.**"Handling Selfishness in MANETs – A Survey", Vol. 3, Issue 11, November 2014.

[3]. **BathiSrikanth** "Detecting Selfish Nodes in MANETs", June 2014.

[4]. **K.Aathi Dharshini, C.Susil Kumar, E.BabuThirumangaiAlwar**."Derivative Threshold Actuation For Single phase wormhole detection with reduction false alarm rate", Vol.5, No.1/2/3, May 2014.

[5]. **Ms. I.Shanthi, Mrs. D. SornaShanthi.**"Detection of false alarm in handling of selfish nodes in MANET with congestion control", Vol. 10, Issue 1, No 3, January 2013.

[6]. **Karthik M, Jyothish K John, Leenu Rebecca Mathew, Tibin Thomas,** "Detection of False Alarm in Handling of Selfish Nodes in Mobile Ad Hoc Networks", Vol. 1, Issue 10, 2013.

[7]. **Gaurav, Naresh Sharma, HimanshuTyagi**."False Node Detection Algorithm in Cluster Based MANET",Volume4, Issue 2, February 2014.

[8]. **Yian Huang WenkeLee .**"A Cooperative Intrusion Detection System for Ad Hoc Networks" Proc. of the 1st ACM workshop on Security of ad hoc and sensor networks, Pages 135-147,2003.

[9]. **Farhan Abdel-Fattah ZulkhairiMd, DahalinShaidahJusoh**. "Dynamic Intrusion Detection Method for Mobile Ad Hoc Network Using CPDOD Algorithm", IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010.

[10]. **YugandharaBhalkar, UjwalaChaskar, VanashriChaudhari,ChandrashekharGirigosavi**."Eliminating Selfishness to Improve Replica Allocation over MANET's",Volume 4, Issue 10, October 2014.

[11]. **Y. Xiao, X. Shen, and D.-Z.Du** ."A Survey on Intrusion Detection in Mobile Ad Hoc Networks", (Eds.) pp. 170 – 196 °c 2006 Springer.

[12]. **S.Prabhavathi, Ms.R.Bharathi** ."Identifying and handling of false alarm in selfish replica" , Volume 5, Issue 2, February-2014 375.

[13]. **P.BakeyaLakshmi, Mrs.K.Santhi**."A survey on intrusion detection on MANET",Volume 1, Issue 5, October-2012.

[14]. **K.Aathi Dharshini, C.Susil Kumar, E.BabuThirumangaiAlwar.**"Derivative threshold actuation for single phase wormhole detection with reduced false alarm rate", Vol.5, No.1/2/3, May 2014.

