Mitigation of Selfish Node Attacks In Autoconfiguration of MANETs

Reshmi.T.R[1], Shymala L[2], Sandhya.M.K[3]
[1, 2] School of Computing Science and Engineering, VIT University, Chennai, India
[3]Department of Computer Science and Engineering, Meenakshi Sundararajan Engineering College, Chennai, India

Article Info

Article history:

Received Dec 19, 2017
Revised Mar 24, 2018
Accepted May 11, 2018

Keyword:

Addressing
Autoconfiguration
MANETs
Mean Value Analysis
Selfish nodes

ABSTRACT

Mobile ad-hoc networks (MANETs) are composed of mobile nodes connected by wireless links without using any pre-existent infrastructure. Hence the assigning of unique IP address to the incoming node becomes difficult. There are various dynamic auto configuration protocols available to assign IP address to the incoming nodes including grid based protocol which assigns IP address with less delay and low protocol overhead. Such protocols get affected by presence of either selfish nodes or malicious nodes. Moreover there is no centralized approach to defend against these threats like in wired network such as firewall, intrusion detection system, proxy etc. The selfish nodes are the nodes which receive packet destined to it and drop packet destined to other nodes in order to save its energy and resources. This behavior of nodes affects normal functioning of auto configuration protocol. Many algorithms are available to isolate selfish nodes but they do not deal with presence of false alarm and protocol overhead. And also there are certain algorithms which use complex formulae and tedious mathematical calculations. The proposed algorithm in this paper helps to overcome the attack of selfish nodes effect in an efficient and scalable address auto configuration protocol that automatically configures a network by assigning unique IP addresses to all nodes with a very low protocol overhead, minimal address acquisition delay and computational overhead.

Corresponding Author:

Dr.Reshmi T R,
School of Computing Science and Engineering,
VIT University, Chennai, India
Email: reshmi.tr@vit.ac.in

1. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) are dynamic ad hoc networks with mobile nodes that self-configure for communication and frequently change the locations due to mobility. The mobile devices in MANETs use wireless connections for communications. The wireless communication can be a Wi-Fi connection, cellular or satellite transmission. MANETs are divided as Pure MANETs and Connected MANETs. Pure MANETs (also known standalone MANETs) are restricted to a local area of wireless devices (such as a group of laptop computers), while Connected MANETs (also known as Internet Connected MANETs) may be connected to the Internet. In local area MANETs, the IP address assigned to the nodes need to be locally unique. In Internet Connected MANETs the IP address assigned to nodes must be globally unique.

In MANETs, nodes are not assigned with static IP address due to the dynamic topology of the network. The centralized approach like Dynamic Host Configuration Protocol (DHCP) requires servers to serve multiple requests and assign IP addresses to the requesting nodes. But as these servers consume high battery consumption and resources, the centralized approach is not suitable for MANETs. To assign unique IP address for the nodes, Distributed dynamic addressing schemes are more suitable in MANETs. In these schemes each of the nodes is assigned to do the addressing and hence every node shares the workload. The performance of address assigning is affected by prevalence of selfish nodes in the network. In some scenarios, the nodes which detect duplicate addresses and find unique IP address to newly entering nodes behave in selfish manner to save energy, bandwidth and power. This deteriorates the performance of the address configuration protocols. This paper presents a dynamic addressing protocol called Trust Based Service Discovery Protocol which finds the trusted nodes as configuring nodes to avoid the packet drops during the configuration process. Thereby the proposed protocol improves the Quality of Service (QoS) of the MANETs by reducing the delay in service discovery and participation.

In IP-based networks, uniqueness of the addresses is the most important requirements forth nodes to participate in unicast communications and routing. Often nodes assume to have unique IP addresses pre-configured before communication. However, this is not the scenario and is not easily achieved in MANETs. Most of the existing address allocation schemes in MANETs use a flooding technique for address solicitation and duplicate address detection. As a result, addressing schemes are prone to several types of security threats. In this paper, we focus on the selfish node attacks during autoconfiguration or addressing of nodes in MANETs. The paper presents a grid-based distributed dynamic IP configuration scheme that securely allocates IP addresses to the authorized nodes without flooding the network. The scheme initially makes each node to acquire unique IP addresses from specialized nodes called Distributed Duplicate-IP address Detection Servers and assign these addresses to the new nodes. The proposed scheme ensures security against the associated threats with dynamic IP allocation protocol. It also efficiently handles the network partitioning and merging and also reduces address conflicts.

The paper is organized in to four sections. The first section describes the working of the dynamic addressing protocols. The second section discusses about the proposed Mean Value Analysis (MMVA) algorithm for trust evaluation of nodes in network. The third section discusses about the analysis of the protocol messages with a case study. The section 5 presents the performance analysis and simulation results to show that the proposed addressing scheme has added more security features compared to an existing dynamic address allocation schemes. Finally the section 6 discusses the conclusion derived on the analysis of the protocol.

2. RELATED WORK

There are different approaches for auto-configuration in MANETs. The characteristic features of the addressing schemes differ in some aspects, as follows.

Günes and Reibel [1] proposed a stateful protocol which uses a centralized allocation table. This protocol is called in Centralized Auto-configuration (CAC) [2]. The main idea of the approach is to dynamically select one of the nodes to maintain the list of all available nodes in MANET. This node performs the address assignment in the same way as an address configuration server. This scheme uses technique similar to DHCP auto-configuration protocol. But the protocol is more prone to attacks or performance deterioration if the elected node behaves as selfish node. Vaidya [3] proposed a stateless protocol which uses a DAD mechanism integrated with the routing protocol. This mechanism called weak DAD (WDAD) uses a key generated during node auto-configuration and uses it to check whether more than one node have selected the same IP address resulting IP conflict in network. But keys used in the technique impose overhead on the routing protocol. Thus, there is a trade-off between reliability and overhead in WDAD.

Sun and Belding-Royer [4] proposed a hybrid protocol that uses of a query-based *DAD* mechanism in combination with a centrally maintained allocation table. The protocol enables nodes to select unique IP addresses, and is able to detect address duplicates after network merges. The information of the network is maintained by the Address Authority (AA) to compute the Network prefix. The node selects an address by itself and verifies its uniqueness by sending an Address Request (AREQ) with the query-based DAD. So the nodes assigned with IP addresses disputes an Address Reply (AREP) to claim the ownership of the address. The protocol performs well in the network partition and merging. But the resource consumption for maintaining the allocation table is a drawback of the scheme.

Weniger [5] proposes a hybrid protocol which makes use of *PDAD* mechanism in conjunction with a distributed maintenance of a common allocation table. This protocol is called The Passive Auto-configuration for Mobile Ad Hoc Networks (PACMAN), the protocol uses cross layer information derived from ongoing routing protocol traffic. Using this nodes passively collect information about already assigned addresses and detect address conflicts. This protocol supports frequent network partitioning and merging, also has a very low protocol overhead. Also it avoids to actively synchronizing allocation tables, hence no additional bandwidth is consumed.

Syed et al. [6] presents an efficient and scalable address auto configuration protocol that automatically configures a network by assigning unique IP addresses to all nodes with a very low protocol overhead and minimal acquisition delay. The Duplicate-IP Address Detection Servers are used to ensure the uniqueness of an IP address during IP address assignment session. In contrast to some other solutions, the proposed protocol does not exhibit any problems pertaining for leader election or centralized server-based solutions. Furthermore, grid based hierarchy is used for efficient geographic forwarding as well as for selecting DuplicateIP address Detection Servers.

There is an emergent security problem related to mobile ad hoc network (MANET).This new problem is selfishness on packet forwarding due to the resource limitation of nodes in the ad hoc network. To save its energy, a node behaves selfishly, by utilizing the forwarding service of other nodes, but it does not forward packets for them. This makes delay in auto-configuration of MANETs. It is important to detect selfish nodes in ad-hoc network. Detection of the misbehavior nodes requires many packets lost detections with respect to time. A gradual solution to detect selfish nodes in mobile ad-hoc networks as follows. Enrique Hern´andez-Orallo proposed [6] an Improving Selfish Node Detection in MANETs using a Collaborative Watchdog. In this approach nodes send the selfish node information upon contact with other nodes rather than the promiscuous hearing assumption of the other cooperative methods. The performance of the model is improved over with the performance model developed using Continuous Time Markov Chain. But the selfish node detection time and protocol overhead is high in this technique.

ReshmaLill Mathew proposed a method for detecting Selfish Nodes in MANETs using Collaborative Watchdogs [7]. This paper uses a watchdog system with a log file. This will perform the checking of selfish node only at a particular time and saves the time. The mechanism behind this watchdog system is that, it will overhear when a node sent a packet to its neighbour then the node listen to the neighbour's communication. If the neighbour didn't forward the same packet to its next hope node within a period it was regarded as misbehaving. By this way a node could record the successful and failed history of its next hop. The proposed system detects the selfish node in an accurate way. It won't allow a false negative and also can reduce the false detection. False negative can make a node to be a selfish one which in real won't be such. This decision will results in a network where selfish nodes won't be detected and also the nodes which are not a selfish one will be treated as a selfish one.

Reshmi and Murugan proposed an Application of Fuzzy Sets for Isolating Selfish nodes by Trust Evaluation during Auto-configuration and Service Establishment in MANETs [8]. In this paper fuzzy system is developed in dynamic Distributed Stateful Auto-configuration to isolate selfish nodes in MANETs. Fuzzy sets based on simple rule set are used to prevent the participation of selfish nodes in network address assigning process. The Mean value analysis (MVA) tool is used to analyse traffic behaviours and performance in closed networks. Though the paper improves the network performance metrics like network throughput, network response time and packet drops, but it needs focus on quality of service and network security. Also the logic introduced in this paper has not done to hybrid auto-configuration.

Debdutta Barman Roy proposed a Mobile agent based detection of selfish node in MANET [MADSN] [9]. The approach uses a set of mobile agent (MA) that can move from one node to another node within a network. This as a whole reduces network bandwidth consumption by moving the computation for data analysis to the location of the intrusion. The mobile agents travel through the network, gathering vital information is then processed by the mobile agents themselves. As the computation overhead of the algorithm is less, the computation complexity of the mobile agent will be reduced. The computation is done by mobile agent when the source node notices that the destination node does not respond in correct time. Mobile Ad hoc Network (MANET) is highly vulnerable to attacks due to the open medium dynamically changing network topology, co-operative algorithm, lack of centralized monitoring and management point.

Charlie Obimbo proposed an Intrusion detection system for MANET [10] which introduces an enhancement of the watchdog/path rater form of intrusion detection in mobile ad-hoc network(MANET).The participating nodes are allowed to listen the nodes that they have conveyed messages to, in promiscuous mode. If within a certain time frame the message is not relayed, then the node is suggested to be tagged as a misbehaviour node. Watchdogs run on each node when a node forwards the packet. The watchdog does this by listening in promiscuous mode to the next nodes transmission. If the next node does not forward the packet, then it is considered to be the misbehaving and is reported. This is done by sending an alarm message to the other nodes on its friend's list. Path rater module uses the information generated by watchdog to select a better route to deliver the packets, avoiding the selfish nodes. The watch dog and path rater approach the IDS overhear neighbour's packet transmission promiscuously and notify misbehaviour to the source node by sending a message. Though the scheme is easier to implement it depends on promiscuous listening that may results false identification.

Jae-Ho Choi proposed a Handling Selfishness in Replica Allocation over a Mobile Ad Hoc network [9]. This paper uses novel replica allocation techniques to handle the selfish replica allocation appropriately. Every node in a MANET calculates credit risk information on other connected nodes individually to measure the degree of selfishness. Since traditional replica allocation techniques failed to consider selfish nodes, the paper proposed novel replica allocation techniques. The simulation results show that the proposed strategies outperform existing representative cooperative replica allocation techniques in terms of data accessibility, communication cost, and query delay. But it is not consider about false alarms in selfish replica allocation.

There are many autoconfiguration schemes [2-9] that meets the basic requirements of the addressing protocols. The security issues in these schemes are still a growing trend of research. The security threat called selfish node attacks and its impact in autoconfiguration scheme is focused in this paper.

3. PROPOSED WORK

The proposed protocol deals the mitigation of selfish nodes in addition to the common features of the address configuring protocol in MANETs.

3.1. Basic Idea of the Protocol

The network topology is divided in to grids (named as order 1, order 2 etc.) based on number of nodes. When the node enters in to MANETs, it determines its position using GPS and locates itself in order-1 square. Each square consists of disjoint block of temporary IP address pool ranges from 1 to 2048. The newly entering node randomly chooses conflict free IP address from the pool. To avoid conflict when two or more number of entering new nodes picks up same IP address from the pool, nodes runs duplicate detection process in order-1 square using one hop broadcasting message. Receiving NACK message from any nodes, new node gives up temporary IP address and randomly chooses another IP address from the pool. Based on Temporary IP address assigned to nodes, duplicate detection servers (DDSs) for every order square are selected to run duplicate detection algorithm.

After resolving temporary IP address, a node randomly chooses a real IP address. It then makes queries through QUERY messages to DDSs for the chosen real IP address in each order squares. If an entry is found in the Duplicate-IP address Detection Table (DDT) of any of those DDSs, the corresponding DDS immediately informs the node using NACK message. The node then chooses another real IP address randomly and the same process is repeated again after a random amount of time. The QUERY messages are sent iteratively. At first, the node sends queries to DDSs in Order-1 squares. If IP address conflict is detected in any Order-1 square, there is no need to send queries in peer Order-2 squares. In general, when an IP address conflict is detected in Order-n Square, there is no need to send any further query to Order-(n +1) square or higher Order peer squares. If no conflict is detected in any of the DDSs at any Order, no reply is sent to the requesting node. Therefore, if the node receives no NACK message within a timeout interval, it assumes that the real IP address is conflict-free and finalizes this IP address as its real IP address.

The protocol reduces flooding of message in the network there by reduces protocol overhead and address acquisition delay. But the protocol is more prone to prevalence of selfish nodes. If the nodes which are selected for the DDSs behave in selfish manner, then the overall performance of protocol gets affected. So, the proposed algorithm in this paper helps to mitigate the above said problem. The algorithm uses trust level to isolate the selfish nodes. This section explains the results of research and at the same time is given the comprehensive discussion. Results can be presented in figures, graphs, tables and others that make the reader understand easily [1, 5]. The discussion can be made in several sub-chapters.

3.2. Trust Based Dynamic Distributed Hybrid IP Addressing Protocol for MANETs

The protocol is the enhancement of Scalable Address Auto-configuration in Mobile Ad Hoc Networks proposed by Syed et al [5]. The protocol is more focus on mitigation of selfish nodes effect in address configuration thereby improving the performance of the network like address acquisition delay, protocol overhead and pocket losses. This improves QoS of the network.

3.2.1. Mean Value Analysis (MVA) Algorithm

Mean value analysis (MVA) is an efficient algorithm that allows us to analyse product form queuing networks and obtain mean values for response times, throughputs, information about utilization and degree of multiprogramming of the system node. The efficiency comes with a price. Mean value analysis (MVA) is a recursive technique for computing expected queue lengths, waiting time at queuing nodes and throughput in equilibrium for a closed separable system and open system. It is based on Schweitzer’s approximation. This analysis is more suitable for MANETs which are closed system in nature. In this paper the analysis is used to derive the nodes performance metrics of network such as node utilization and node capacity which are required to analyze the performance metrics of the network.

Table 1Description of Notation used in Algorithm

Notation	Description
Si	Service time taken by ith node on each visit of the other node
Vi	Number of visits to the ith node
X	Network throughput
Ui	Utilization of the ith node
Ci	Node Capacity
TL	Trust Level of the node

The parameters which are used by mean value analysis are as follows:

1. Throughput: (X): In communication networks, it is defined as the average rate of successful message delivery over a communication channel. This data must be delivered over a physical or logical link, or pass through a certain network node.
2. Service time (Si): It is the time taken by ith node on each visit of the other node. It is calculated by subtracting start time from end time of the node response to the other node.
3. Visit Time (Vi): It is defined as Number of visits to the ith node. It is counted by the every node in the network to its neighbor nodes.

The following formulae are used to calculate node capacity and node utilization.

$$Ci = XVi$$

$$Ui = XViSi$$

3.2.2. Selfish Node Isolation Using Trust Level

The trust level is divided into three and four levels such as low, medial and high. The range of trust levels are as follows.

For Node capacity:

LOW=L=0-0.39
MEDIUM=M=0.40-0.69

HIGH=H=0.70-1.0

For Node Utilization:

LOW=L=0-0.09
MEDIUM =M=0.1-0.19
HIGH =H=0.2-0.59

VERY HIGH=VH=0.6-1

Table 2. Trust level evaluation with rules set

Ci/Ui	L	M	H	VH
L			L	
M	L		M	H
H	L	M	H	VH

4. PERFORMANCE ANALYSIS

The proposed autoconfiguration scheme and the existing schemes are implemented in Network Simulator 2 (NS2) to analyse, compare and study the performance.

The graph showing different network parameters are shown below. The results show that overall performance of the network is improved when the low trust level nodes are neglected during address duplication process.

The results showed in Figure 1 shows the average address acquisition delay in various scenarios. The performance of the address acquisition delay has been improved when the auto configuration process uses the node with medial and high trust level for address duplication detection. While comparing it with the existing watchdog it can be understood that it is improved. The average number of packet losses during auto configuration is shown in Figure.2. When the nodes with low trust level are neglected during address assigning process the number of packet losses has become reduced. Moreover the packet losses are less when compared with the watchdog. The results in Figure.2 show that average protocol overhead in various scenario. Though it initially decreases for small number of nodes it increases when the number of nodes increases. But it value is less compared with existing watchdog.

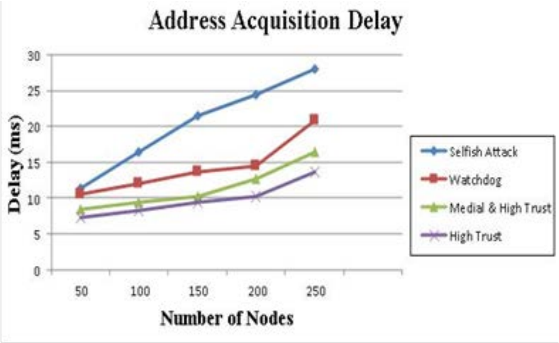

Figure 1. Address Acquisition Delay in various scenarios

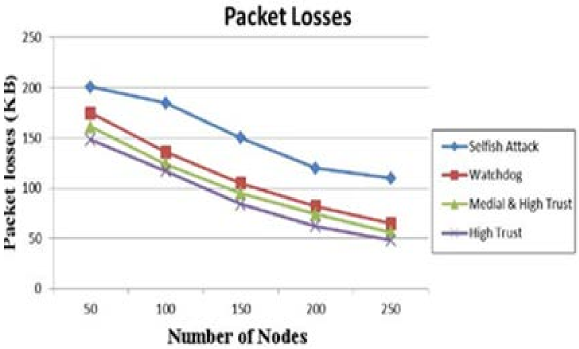

Figure 2. Graph of protocol overhead in various scenarios

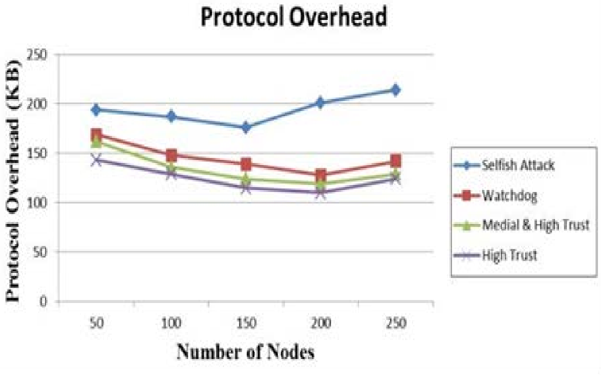

Figure.3 Graph of protocol overhead in various scenarios

5. CONCLUSION

The Protocol uses mean value analysis for the selection of Distributed Duplicate-IP Detection Servers (DDSs) which are required for ensuring the uniqueness of chosen IP addresses instead of flooding mechanism. The every node in the network calculates the parameters need for the mean value analysis. No special hardware is required to monitor the neighboring nodes whether the nodes behave in selfish manner. Also the analysis requires simple formulae and low mathematical calculation. The simulation results conclude that the protocol reduces overhead, address acquisition delay, and packet losses thereby improving the overall performance of the network. Though the protocol prevents attack of selfish nodes, it is more vulnerable to the attack of malicious and helpless nodes.

REFERENCES

[1] N. H. Vaidya, “Weak Duplicate Address Detection in Mobile Ad Hoc Networks”, Proc. ACM MobiHoc 2002, Lausanne, Switzerland, June 2002, pp. 206–16.

[2] K. Weniger and M. Zitterbart, "Address Autoconfiguration on Mobile Ad Hoc Networks: Current Approaches and Future Directions", IEEE Network, vol. 18, no. 4, pp. 6--11, July/August 2004.

[3] Y. Sun and E. M. Belding-Royer, “Dynamic Address Configuration in Mobile Ad Hoc Networks”, UCSB tech. rep. 2003-11, Santa Barbara, CA, June 2003.

[4] M. Günes and J. Reibel, “An IP Address Configuration Algorithm for Zeroconf Mobile Multihop Ad Hoc Networks”, Proc. Int’l. Wksp. Broadband Wireless Ad Hoc Networks and Services, Sophia Antipolis, France, Sept. 2002.

[5] Syed Rafiul Hussain, Subrata Saha and Ashikur Rahman, “SAAMAN: Scalable Address Auto configuration in Mobile Ad Hoc Networks”, Distributed Computing, 2010.

[6] Natalia Castro Fernandes, Marcelo Duffles Donato Moreira, and Otto Carlos Muniz Bandeira Duarte, “An Efficient and Robust Addressing Protocol for Node Auto configuration in Ad Hoc Networks”, IEEE/ACM Transactions On Networking, 2013.

[7] Zohra Slimane, Abdelhafid Abdelmalek, Mohamed Feham and Abdelmalik Taleb-Ahmed, “Secure And Robust Ipv6 Autoconfiguration Protocol For Mobile Adhoc Networks Under Strong Adversarial Model”, International Journal of Computer Networks & Communications (IJCNC) Vol.3, No.4, July 2011.

[8] Safdar Hussain Bouk and Iwao Sasase, “IPv6 Autoconfiguration for Hierarchical MANETs with Efficient Leader Election Algorithm”, Journal Of Communications And Networks, Vol. 11, No. 3, June 2009.

[9] Jianli Hu, Quanyuan Wu and Bin Zhou, “Secure and Distributed P2P Reputation Management”, Journal Of Communications, Vol. 3, No. 7, December 2008.

[10] Network Simulator: http:///www.isi.edu/nsnam/ns.