World Wide Journal of Multidisciplinary Research and Development

World Wide Journal of Multidisciplinary Research and Development

WWJMRD 2017; 3(6): 92-94
www.wwjmrd.com
Impact Factor MJIF: 4.25
e-ISSN: 2454-6615

Jasmeen Mangat
M.Tech (CSE) Guru Kashi University, Talwandi Sabo, Bathinda, Punjab, India

Jaspreet Kaur
Assistant Professor Guru Kashi University, Talwandi Sabo, Bathinda, Punjab, India

Correspondence:
Jasmeen Mangat
M.Tech (CSE) Guru Kashi University, Talwandi Sabo, Bathinda, Punjab, India

A Novel Technique to Detect and Prevent Spoofed Flooding Attack in MANETs

Jasmeen Mangat, Jaspreet Kaur

Abstract
The mobile nodes within the MANET can freely join and leave the network. The nodes within network may also behave maliciously. In past many researchers have focused to detect or prevent an attacker showing the single abnormal behavior. However if any adversary or malicious node uses two different kinds of attacks at same time, its detection or prevention is found rarely in literature. This paper considers a new form of attack, i.e. Spoofed Flooding Attack. This attack is advanced form of flooding attack in which the attacker node also practices the node ID capture attack as well. The attacker node clones the ID of some genuine node and floods the network with RREQ packets. This paper presents a scheme to detect and prevent such kind of attack. The scheme has been implemented in NS2. The performance has been analyzed based on remaining energy of the network, throughput and packet delivery ratio.

Keywords: MANETs, Spoofed flooding, packet delivery ratio, throughput

Introduction
Security is more challenging to maintain in MANETs due to their vulnerability, than wired networks. The use of wireless links renders an ad hoc network susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay and distortion [8]. The first step towards developing good security solutions is to understand possible form of attacks. Security of communication in MANET is critical for secure transmission of information. Due to the absence of any central co-ordination mechanism and the presence of shared wireless medium, MANET becomes more vulnerable to digital/cyber-attacks than wired network. The attacks can be internal or external, and according to the behavior of the attack it can be Passive or Active attack. This paper considers a new form of attack, i.e. Spoofed Flooding Attack. This attack is advanced form of flooding attack in which the attacker node also practices the clone attack as well. Therefore, one can say this attack is combination of flooding and clone attack. The attacker node clones the ID of some genuine node and floods the network with RREQ packets.
Section II represents the brief survey about the detection and prevention of the attack in which node ID is captured. Proposed work has been represented in Section III. It gives details about the scheme implemented. The results are shown in Section IV.

Literature Survey
Faizan Khan [2016] in this paper author will concentrate on recognizing the Sybil attack in MANET. It utilizes air medium for correspondence so it is more inclined to the attack. Mobility causes a fundamental issue when we discuss security in Mobile Ad-hoc network. It does not rely on upon fixed design, the nodes are constantly moving in an arbitrary form. Sybil attack is one in which single node display various fake characters to different nodes, which cause destruction. Through simulation, it is shown that this discovery can be finished by utilizing the device NS2.35 [1].

T. Saranya et.al., [2016] In this paper, author propose a lightweight plan to identify the new characters of Sybil attackers without utilizing centralized trusted third party or any additional equipment, for example, directional receiving wires or a topographical situating system. Completely self-organized mobile ad hoc network systems (MANETs) communicate to complex distributed systems that may also be a piece of an enormous complex system, for example, a typical system-of-systems utilized for emergency administration operations.

Because of the complex nature of MANETs and its asset imperative nodes, there has dependably been a need to create lightweight security arrangements. Since MANETs require a one of a kind, particular, and diligent identity per node all together for their security protocol to be practical, Sybil attacks represent a genuine risk to such systems. A Sybil attacker can either make more than one identity on a single physical gadget keeping in mind the end goal to dispatch a facilitated attack on the system or can switch characters keeping in mind the end goal to debilitate the identification procedure, subsequently advancing absence of responsibility in the arrange. Through the simulation author can show that their proposed conspire distinguishes Sybil characters with great exactness even within the sight of mobility [2].

P. Raghu Vamsi and Krishna Kant [2016] proposed a technique for identifying Sybil attack utilizing successive investigation. This technique works in two phases. To start with, it gathers the confirmations by watching neighbouring node exercises. Further, the gathered confirmations are united to give contribution to the second stage. In the second stage, gathered confirmations are approved utilizing the successive likelihood proportion test to choose whether the neighbour node is Sybil or genuine. The proposed technique has been assessed utilizing the system test system ns-2. Re-enactment results demonstrate that the proposed technique is powerful in identifying Sybil attacks with low false positive and false negative rates [3].

Prabhjot kaur et al., [2016] proposed in this paper a work in which they have a tendency to adjust the brought together IDS plan which is based on the abuse detection to recognize the malicious cluster head which has the expectation of bringing about the Sybil attack in the remote sensor system. Work affirm the adequacy of our adjusted IDS regarding the right detection of every single existing attack [4].

K. deepalaskshmi [2015] In this paper, Author introduced a plan that recognizes Sybil identities. Specifically, their plan uses the RSS keeping in mind the end goal to separate between the legitimate and Sybil characters. In the first stage, they illustrate the passage, leave conduct of legitimate nodes and Sybil nodes utilizing simulation, and tried experimentation. Second, we characterize an edge that recognize the threshold and Sybil characters in view of nodes' entry and exit behavior. Third, they describe location edge by joining the RSS information taken from their tried experimentation. Fourth, they assess the plan utilizing broad simulations, and the outcomes demonstrate that it creates around 90% genuine positives (distinguishing a Sybil nodes Sybil) and around 10% false positives (recognizing an ordinary node as a Sybil node) in mobile conditions [5].

Yamini D.Malkhed el at. [2015] proposed a recognition method, which depends on RSS alongside the authentication of node, which will accurately, distinguished the Sybil identity with Higher True Positive. By Authentication implies just genuine gestures are permitted to come into the system. Also Lower-bound identification edge is utilized, and contrast and Received Signal strength value, if the examination is greater than or equivalent to RSS value, then it is a Sybil identity. Generally, it is an authentic node in the system [6].

P.Kavitha el at [2014] proposed a location method, which depends on NDD calculation for distinguishing Sybil attacks. This calculation is utilized to exchange the information from source to goal with no harm or misfortune and additionally each node to have the neighbor's node address. Relies on upon the address the information will be transmitted into right goal [7].

Proposed Work

Initially the proposed work would proceed with the detection of the flooding attack as defined in the existing scheme. The detection scheme for the flooding attack is explained below:

The source node would start with broadcasting of the RREQ packets in the network. This process of forwarding RREQ packets continue until destination is found. In this whole process of forwarding the RREQ packets, if any node tries to flood its neighbors by sending huge number of RREQ packets, the forwarding behavior of the nodes is against the threshold value. If any node is found to forward the more number of RREQ packets than the threshold value, it will be detected.

Once the flooding node is detected, the method to detect the spoofed ID will start in the following way:

After detecting the malicious node by its neighbor, the neighboring node will store the ID and inform the source node about the same. Source will start the fake broadcasting process with destination set as the ID of the malicious node detected in the former steps. If the malicious node has spoofed the ID of some genuine node, then there will be two replies – one from the malicious node and other one from the genuine node. In such a scenario, the malicious node spoofing the ID will be detected and genuine node will not be considered as an attacker node.

Results

The performance of the network was analyzed based on three parameters namely packet delivery ratio, throughput and remaining energy in the network.

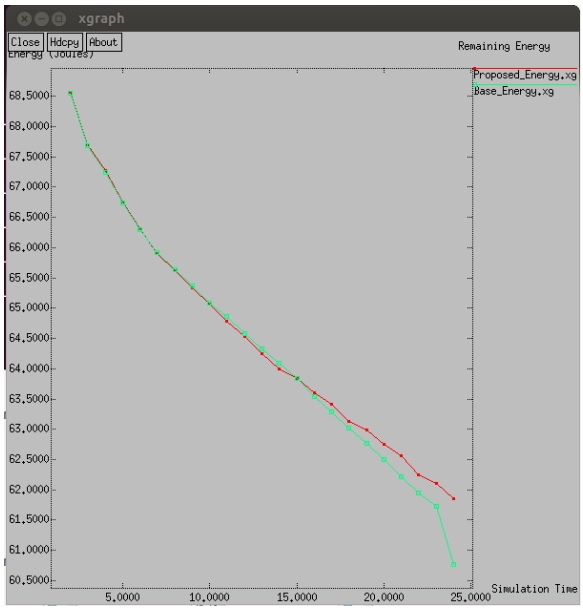

Fig. 1: Comparison of Remaining Energy

This figure shows the remaining energy of the network for proposed scheme and the existing scheme. The value for proposed scheme was higher than the existing scheme, thereby indicating lesser energy consumption.

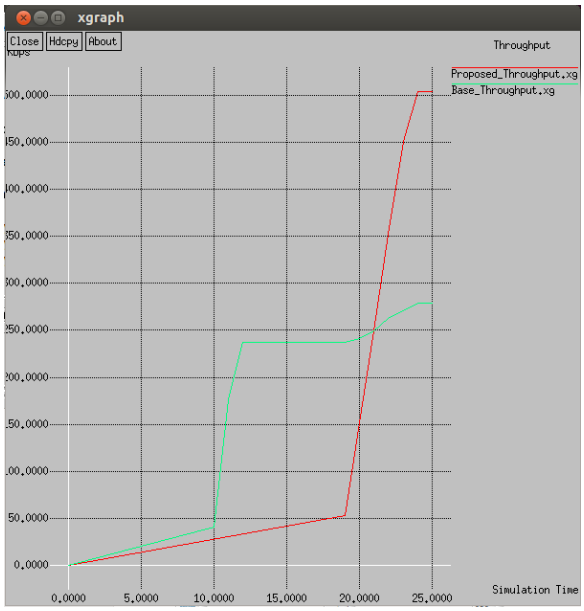

Fig. 2: Throughput comparison

The throughput is quantity of data received at the destination node. The throughput showed higher values for the proposed scheme with the value at 500 Kbps and at 270 Kbps for the existing scheme.

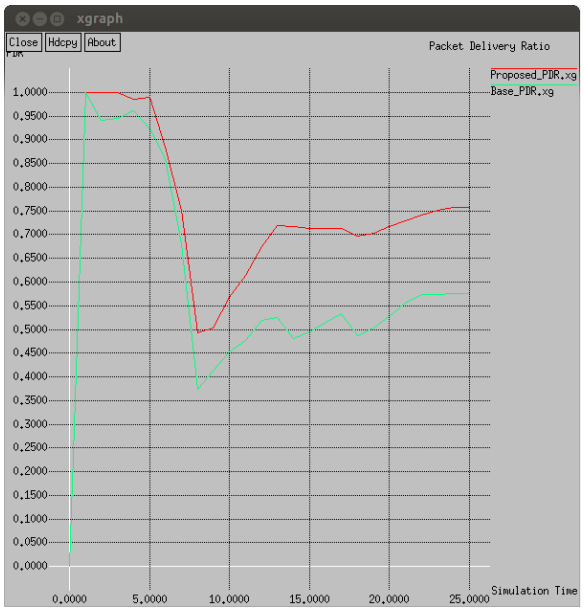

Fig. 3: PDR Comparison

The value of packet delivery ratio for the proposed scheme was approx. 0.75 and for the existing scheme, it was 0.53.

Conclusion

This work aimed to detect and prevent new category of attacks namely spoofed flooding attacks. In this type of attack, the attacker floods the Route Request packets with a spoofed ID. The existing work related to the detection of the flooding attack using the concept of the threshold. It was not including any method to detect the spoofed flooding attack. The performance of both the existing as well as the proposed scheme was analyzed based on packet delivery ratio, throughput and energy consumption of the network. All these parameters showed higher/better values for the proposed scheme. In the existing scheme, genuine nodes are detected as the attacker node since their IDs have been captured and the scheme lacks any procedure to detect spoofed ID. Therefore, every time the source node has to send some data to the destination and it does broadcasting process, the attacker node would come up with new ID and they will flood the network each time and degrade performance of the network.

This category of the attack is new to the mobile ad hoc networks, so in future more energy efficient schemes can be designed to overcome this attack. In addition, we have analyzed the network's performance using three parameters, so in future more parameters can be taken such as delay, bandwidth consumption of the links, etc. to check the effect of the spoofed flooding attack.

References

1. Faizan Khan, Mayuri Sonar, Mosmi Tiwari Vyas, " A Survey Paper on Detection of Sybil Attack in MANET" in International Journal of Computer Networks and Wireless Communications (IJCNWC), Vol.6, No 1, Jan-Feb 2016.
2. T. Saranya, A. Kumarave, "Sybil attack detection in MANETS" in International Journal of Electronics and Communication Engineering Volume 3 November 2016.
3. P. Raghu Vamsi and Krishna Kant, " Detecting Sybil attacks in wireless sensor networks using sequential analysis" in international journal on smart sensing and intelligent systems vol. 9, no. 2, June 2016.
4. Prabhjot kaur, Aayushi Chada, Sandeep Singh, " Review Paper of Detection and Prevention of Sybil Attack in WSN Using Centralized ids" in International Journal of Engineering Science and Computing, July 2016.
5. Mrs. K. Deepalakshmi, Ms. A. Sivasankari, Mrs. B. Arulmozhi, " Sybil Attack Detect in MANETs" in International Research Journal of Engineering and Technology Volume: 02 Aug-2015.
6. Sohail Abbas, Madjid Merabti, David Llewellyn Jones, and Kashif Kifayat," Lightweight Sybil Attack Detection in MANETs", IEEE systems journal, vol. 7, no. 2, June 2013.
7. Yamini D Malkhede, Purnima Selokar "Analysis of Sybil Attack Detection in Mobile Ad hoc Network" Proceedings of 19th IRF International Conference, 1st February 2015, Pune, India, ISBN: 978-93-84209-85-8.
8. Ashwani Garg and Vikas Beniwal, "A Review on Security Issues of Routing Protocols in Mobile Ad-Hoc Networks", in International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE) Volume 2, Issue 9, September 2012.