Journal of Electrical Engineering & Electronic Technology

Opinion Article A SCITECHNOL JOURNAL

Behavioral Model to Detect Anomalous Attacks in Packet Transmission

Peter Henry*

Journal of Electrical Engineering and Technology, University of Rome, Aldo Moro, Roma, Italy

***Corresponding Author:** Peter Henry, Journal of Electrical Engineering and Technology, University of Rome, Aldo Moro, Roma, Italy. E-mail: henrypaul@gmail.com

Received date: 06 June, 2022, Manuscript No. JEEET-22-54785;

Editor assigned date: 08 June, 2022; PreQC No. JEEET-22-54785(PQ);

Reviewed date: 15 June, 2022, QC No. JEEET-22-54785;

Revised date: 13 July, 2022, Manuscript No. JEEET-22-54785(R);

Published date: 29 July, 2022, DOI: 10.4172/jeeet.1000920.

Description

Inside a network environment, packets are the most important in carrying data to perform communication. Such a circumstance is easy to be attacked by an intruder and perform eavesdropping which leads to data loss or duplication or redundancy. Comprehend speaking; packet dropping and modification are the two common attacks that can be easily launched by an adversary to disrupt communication in multi hop networks, specifically mobile ad hoc networks. Hence a remedial approach is proposed to compensate such attacks. A tree based approach is designed to designate the attack in order to identify packet droppers and modifiers. In this direction, it has been assumed that the mobile nodes continuously monitor the behaviors of the forwarding mobile nodes which may be neighbors to determine if their neighbors are misbehaving. To address this problem, a hierarchical method is proposed and detects malicious mobile nodes that drop or modify packets. Extensive analysis and simulations have been conducted to study the performance of attacks with respect to efficiency of the scheme, attack, intruder, behavior, packet dropping and modification. In a wireless ad hoc mobile network, mobile nodes play all the characteristics which include monitor the environment, detect events of interest, produce data, and collaborate in forwarding the data toward a sink, which could be a gateway, base station, storage node, or querying user. Because of the ease of deployment, a mobile ad hoc network is often deployed in a hostile environment to perform the monitoring and data collection tasks.

Dropping and Modification

In such an environment, it certainly lacks physical protection and is subject to node compromise. Due to this compromising behavior by one or multiple nodes, it is possible for an adversary to launch various attacks to disrupt communication. Among these attacks, packet dropping and modifying are the common attacks that highly affect the communication process disruption. It is assumed that the compromised nodes perform drop or modify operation over the packets that they are supposed to forward. To deal with packet droppers, a widely adopted counter-measure is multipath forwarding in which packets is forwarded along multiple redundant paths and hence packet dropping in some but not all of these paths can be tolerated. To deal with packet modifiers, most of existing countermeasures aim to filter modified messages en-route within a certain number of hops. These countermeasures can tolerate or mitigate the packet dropping and modification attacks, but the intruders are still there and can continue attacking the network without being caught. Packet dropping and modification attacks are tolerable by using these existing methods, but the attackers are still there and can continue attacking the network without being caught. It has been considered that mobile nodes continuously monitor the forwarding behaviors of their neighboring nodes to determine their neighboring nodes behavior. In order to identify packet droppers and packet modifiers, the existing approaches can be extended by using the reputation-based IDS mechanisms. While data is in transit, these mechanisms helps and emphasize to detect each forwarding node is trustable or not worthy in terms of behavior.

But the modified packets were not being filtered out and routed because they should be used as evidence to infer packet modifiers; hence, it cannot be used together with existing packet filtering schemes. In our proposal, it has been designed an effective scheme to catch both packet droppers and modifiers within a single module. In this scheme, a routing tree rooted at the sink is first established. When data are being transmitted along the tree structure toward the sink, each packet sender or forwarder adds a small number of extra bits, which is called packet marks, to the packet. The format of the small packet marks is deliberately designed such that the sink can obtain very useful information from the marks. The main advantage of this scheme is to produce mis behavior bad nodes in a network system. A node categorization algorithmic stated to identify nodes that are droppers/modifiers for sure or are suspicious droppers or modifiers. As the tree structure dynamically changes every time interval, behaviors of nodes is observed in a large variety of scenarios. As the information of node behaviors has been accumulated, heuristic ranking algorithm to identify most likely bad nodes from suspiciously bad nodes. This way, most of the bad nodes can be gradually identified with small false positive. In a typical ad hoc network, it is clear that a large number of mobile nodes are randomly distributed in a two dimensional area. Each node generates data periodically and all these nodes collaborate to forward packets containing the data toward a sink. The sink is located within the network itself. Assumed that all nodes and the sink are loosely time synchronized, this is implemented in many of the applications.

Network Topology

Attack-resilient time synchronization schemes, which have been widely investigated in wireless networks, are employed. The sink is aware of the network topology, which can be achieved by requiring nodes to report their neighboring nodes right after preparation. It is observed that the network sink is trustworthy and free of compromise. Therefore, the adversary cannot successfully compromise regular nodes during the short topology establishment phase once the network is positioned. This assumption has been widely used in existing work. After then, the regular nodes can be made as compromised. Compromised nodes may or may not collude with each other. A compromised node can launch the following two attacks. Packet dropping: A compromised node drops all or some of the packets that is supposed to forward. It may also drop the data generated by itself for some malicious purpose such as framing innocent nodes. Packet modification: A compromised node modifies all or some of the packets that is supposed to forward. It may also modify the data it generates to protect itself from being identified or to accuse other nodes. Two techniques exist to improve throughput in any network system that agree to forward packets in between the nodes in the presence of bad nodes. Such problems are proposed with categorization techniques based upon the nodes dynamically measured behavior. The existing system implemented like a watchdog to identify misbehaving nodes including a path rate that helps routing protocols in avoiding such nodes. Through simulation the watchdog evaluations are done. The path rater is implemented using packet throughput, percentage of overhead (routing) transmissions, and the accuracy of misbehaving node detection. Local monitoring has been demonstrated as a powerful technique for mitigating security attacks in multi-hop networks. In this system, nodes overhear partial neighborhood communication to detect mis behavior such as packet drop or delay. However, local monitoring as presented in the literature is vulnerable to a class of attacks that we introduce here called stealthy packet dropping.

Stealthy packet dropping disrupts the packet from reaching the destination by malicious behavior at an intermediate node. However, the malicious node gives the impression to its neighbors that it performed the legitimate forwarding action. Moreover, a legitimate node comes under suspicion. Four ways are used to achieve stealthy packet dropping, none of which is currently detectable. False data injection is a severe attack that compromised nodes moles can launch. These moles inject large amount of bogus traffic that can lead to application failures and exhausted network resources. Existing network security proposals only passively mitigate the damage by filtering injected packets; they do not provide active means for fight back. Here specify that how to locate such moles within the framework of packet marking, when forwarding moles collude with source moles to manipulate the marks. Existing Internet trace back mechanisms do not assume compromised forwarding nodes and are easily defeated by manipulated marks. It is proposed with a Probabilistic Nested Marking (PNM) scheme that is secure against such colluding attacks. No matter how colluding moles manipulate the marks, PNM can always locate them one by one. Nested marking is proved both sufficiently and necessarily to resist colluding attacks. PNM also has fast-trace back within about 50 packets; it can track down a mole up to 20 hops away from the sink. This virtually prevents any effective data injection attack moles will be caught before they have injected any meaningful amount of bogus traffic.