IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 10, Issue 1, Ver. 1 (Jan - Feb. 2015), PP 05-14
www.iosrjournals.org

Behavioral Model to Detect Anomalous Attacks in Packet Transmission

Suhasini Sodagudi, Prof. Rajasekhara Rao Kurra,
Associate Prof, Dept of IT, VRSiddharthaEngg College, Vijayawada-07, A.P
Email :ssuhasini09@gmail.com
Dean, Sri Prakash college of Engg, Tuni, Sri Prakash College of Tech., Rajahmandry, AP-533401,
Email :krr@sriprakash.org
Krr_it@yahoo.co.in

Abstract: *Inside a network environment, packets is 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/duplication/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.*

Keywords: *attack, intruder, behavior, packet dropping, modification*

I. Introduction

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. 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 [1]. 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[2]. To deal with packet modifiers, most of existing countermeasures aim to filter modified messages en-route within a certain number of hops [3]. 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 attackersare 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. Recently, Ye et al. proposed a probabilistic nested marking (PNM) scheme [5] with the reputation based system. 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 misbehavior bad nodes in a network system. A node categorization algorithmis stated to identify nodes that are droppers/modifiers for sure or are suspicious droppers/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 [6]. 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 [7].

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 [8]. 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.

II. Literature Survey

Two techniques exist to improve throughputin any network system that agreeto 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 [3]. The existing system implemented like a watchdogto identify misbehaving nodes including a path raterthat helps routing protocols in avoiding such nodes. Through simulation the watchdog evaluations are done. The path rater is implemented using packet throughput, percentageof overhead (routing) transmissions, and the accuracy ofmisbehaving node detection [2]. When used together in a networkwith moderate mobility, the two techniques increasethroughput by 17% in the presence of 40% misbehavingnodes, while increasing the percentage of overhead transmissionsfrom the standard routing protocol's 9% to 17%. Duringextreme mobility, watchdog and path rater can increasenetwork throughput by 27%, while increasing the overheadtransmissions from the standard routing protocol's 12% to24% [4].

Local monitoring has been demonstrated as a powerfultechnique for mitigating security attacks in multi-hop networks. In this system, nodes overhear partial neighborhoodcommunication to detect misbehavior such as packet drop or delay.However, local monitoring as presented in the literature isvulnerable to a class of attacks that we introduce here calledstealthy packet dropping. Stealthy packet dropping disrupts thepacket from reaching the destination by malicious behavior at anintermediate node [3]. However, the malicious node gives theimpression to its neighbors that it performed the legitimateforwarding action. Moreover, a legitimate node comes under suspicion. Four ways are used to achieve stealthy packetdropping, none of which is currently detectable. A protocol called MISPAR based on local monitoring is used to remedy eachattack. It presents two techniques – having the neighbors maintainadditional information about the routing path, and adding somechecking responsibility to each neighbor.

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 [3]. 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 [5]. 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.

Selective forwarding attacks may corrupt some missioncriticalapplications such as military surveillance and forestfire monitoring. In these attacks, malicious nodes behavelike normal nodes in most time but selectively dropsensitive packets, such as a packet reporting the movementof the opposing forces. Such selective dropping is hard to detect [6]. It has been proposed that a lightweight securityscheme for detecting selective forwarding attacks. Thedetection scheme uses a multi-hop acknowledgement techniqueto launch alarms by obtaining responses from intermediatenodes. This scheme is efficient and reliable in thesense that an

intermediate node will report any abnormalpacket loss and suspect nodes to both the base station andthe source node. To the best of knowledge, here presents a detailed scheme for detectingselective forwarding attacks in the environment of networks. The simulation results show that even when thechannel error rate is 15%, simulating very harsh radio conditions,the detection accuracy of the proposed scheme isover 95%.

In a large-scale network individual nodes are subject to security compromises [7]. A compromised node caninject into the network large quantities of bogus sensing reportswhich, if undetected, would be forwarded to the data collectionpoint (i.e. the sink). Such attacks by compromised nodes cancause not only false alarms but also the depletion of the finiteamount of energy in a battery powered network [7]. In this paper wepresent a Statistical En-route Filtering (SEF) mechanism that candetect and drop such false reports. SEF requires that each sensingreport be validated by multiple keyed message authenticationcodes (MACs), each generated by a node that detects the sameevent. As the report is forwarded, each node along the wayverifies the correctness of the MACs probabilistically and dropsthose with invalid MACs at earliest points. The sink further filtersout remaining false reports that escape the en-route filtering. SEFexploits the network scale to determine the truthfulness of eachreport through collective decision-making by multiple detectingnodes and collective false-report-detection by multiple forwardingnodes [5]. Our analysis and simulations show that, with an overheadof 14 bytes per report, SEF is able to drop 80-90% injected falsereports by a compromised node within 10 forwarding hops, andreduce energy consumption by 50% or more in many cases [6].

III. Proposed Approach

The related work in developing the implementation standards included My Eclipse which incorporates today's most innovative open-standard technologies (of course including the Eclipse platform) to provide a development environment for J2EE WEB, XML, UML and databases and a wide array of application server connectors to streamline development, preparation, testing and portability. My Eclipse is a commercial available Java EE and Ajax IDE created and maintained by the company Genuitec, a founding member of the Eclipse Foundation. Behavior based anomaly detection model is proposed to identify the packet droppers, modifiers attack in a MANET. This model reflects in designing a system that consists of a network whose lifetime is divided into rounds with virtualized nodes. Each node sends and forwards data via a routing tree which is implicitly agreed with the sink within each round. The routing tree changes in each round. After the sink has received the packet lists from all nodes, it sends out a message to announce the start of the first round, and the message is forwarded hop by hop to all nodes in the network. An effective scheme called “PFMDA (Packet Forwarding, Modifier and Droppers Attack)”as is a part of our proposed system to catch both packet droppers

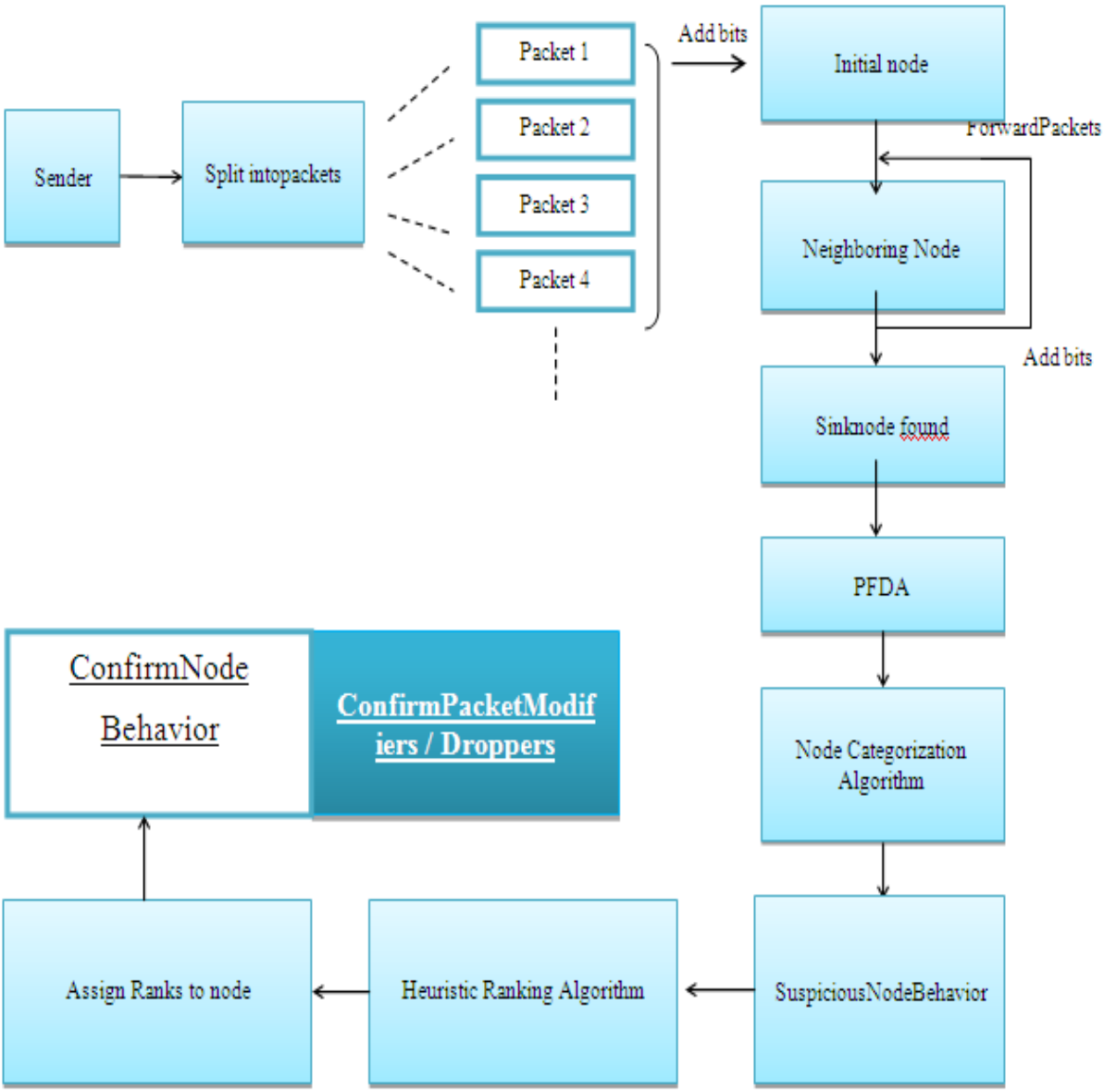


Figure 1. Flow diagram of PFDA system

and modifiers. In this scheme, a routing tree rooted at the sink is first established. When data are 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 sink can figure out the dropping ratio associated with every node, and then runs Node categorization algorithm to identify nodes that are droppers/modifiers for sure or are suspicious droppers/modifiers. Specifically, based on the packet marks, the sink can figure out the dropping ratio associated with every node, and then runs node categorization algorithm to identify nodes that are droppers/modifiers for sure or are suspicious droppers/modifiers. As the information of node behaviors has been accumulated, the sink periodically runs 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 [3]. In PFDA (Packet Forwarding, Modifier and Droppers Attack)" scheme a routing tree rooted at the sink is first established. When data are 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.

Step 1. Take the input information from the sink node
Step 2. Implement "Node Categorization Algorithm" to identify the suspicious nodes
Step3. Implement "Heuristic ranking method" to confirm the node as either "Good/Bad".
Step 4.Use counter measures to confirm that the packets are modified or dropped

Figure2. Algorithm steps in proposed PFDA scheme

The proposed scheme consists of a system initialization phase and several equal-duration rounds of intruder identification phases.A routing tree rooted at the sink is first established. When data are 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 sink can figure out the dropping ratio associated with every node, and then identify nodes t are droppers/modifiers for sure or are suspicious droppers/modifiers. Now it is possible for the sink to have estimation on the dropping ratio. This behavior information is accumulated by the sink periodically to identify most likely bad nodes from suspiciously bad nodes. [2]This way, most of the bad nodes can be gradually identified with small false positive.. The system designed consists of a process with the lifetime of the network divided into rounds with nodes. Once the sink receives the packet lists from all the nodes, it sends out a message indicating the start of the round, is forwarded hop by hop to all nodes in the network.

Node Categorization Algorithm - Link Configuration
In this configuration nodes are configured based on number of nodes in group. Create the network group by connecting nodes to sink. Link configuration means connecting the nodes and intermediate nodes to the sink.

Sender Nodefunctionsinclude :

- Packet Splitting- In this packet splitting sender selects the file which is to be sent. And then it split into the number of packets based on the size for adding some bits in it.
- Send Packets to Intermediate- Encrypts all the spitted packets. And then sender adds some bits to each encrypted packets before sending that. Bit Addition for each packet is identification for sender. After adding of bits to each packet, it sends the packets to the nearest node or intermediate node.

Intermediate Node functionsinclude :

- Send Packets to Sink-At this intermediate node, the intermediate node receives Packets from the sender. After receiving all packets from sender, it encrypts all packets again for authentication. Before sending to sink, intermediate add some bits to each packet for node identification. After adding some bits from intermediate, it sends all packets to the sink.
- Modify or Drop-Before sending all packets to the sink, packets dropping or packets modifying may be occur at the intermediate node.

In each round, data is transferred through the routing tree to the sink. Each packet sender adds a small number of extra bits to the packet and also encrypts the packet. When one round finishes, based on the extra bits carried in the received packets, the sink runs a node categorization algorithm to identify nodes that are bad & suspiciously bad. The sink determines the dropping ratio associated with every node, and then runs Node categorization algorithm to identify nodes that are droppers/modifiers for sure or are suspicious droppers/modifiers.

[1]Likewise the information of node behaviors is cumulated. Now these nodes are called as "bad nodes" only by a suspicion.

Step 1 : Link Configuration - nodes are configured based on the input.
Step 2 : Create the network by connecting nodes to sink.
Step 3 : Select the text file to import into the network
Step 4 : Split the file into packets and append bits in it.
Step 5 : Perform encryption for all the spitted packets.
Step 6 : Append unique packet marks to each encrypted packets before sending.
Step7: Transmit the packets to the neighboring/nearest/intermediate node.
Step 8 : Once the intermediate node receives Packets from the sender, it encrypts all packets again for authentication.
Step 9 : Append packet marks to each packet for the purpose of node identification
Step 10: Transmit all packets to sink

Figure 3.Detailed steps in Node configuration module of PFDA scheme

Hence there is a need to prove these suspicious bad nodes as really bad nodes. From figure 2, it is clear that the sink has collected information about node behaviors in different routing topologies. This information is passed to heuristic method, second part in the proposed system. The algorithm shown in figure identifies bad nodes keeping in view of the changing topologies in the MANET. For this to prove, Heuristic ranking algorithm

is designed to identify most likely bad nodes from suspiciously bad nodes.[5] The algorithm depicted in figure 2 is executed by the sink since the assumption taken is that sink can never be bad node. In this manner, most of the bad nodes are identified with small false positive.

Step1 : Sink after receiving the packets from the sender, verifies them whether are dropped or modified or not.
Step 2 : Identify the modifiers in the process based on the bit identification.
Step 3 : Sink decrypts all packets
Step 4 : If no modified / dropped packets found then merge all packets. Else if there is any modification or drop of packets in node it assumes negative value for modifier or dropper.
Step 5 : Sink receives the original file.

Figure 3. Heuristic Ranking Algorithm of PFMDA

The nodes behavior is monitored to identify the anomalous activity in the network. The anomalous behavior is found to be a point based rather than collective or contextual. Modern technology implementation using My Eclipse is adopted. Hence, a single approach is proposed and was successful to detect three attackers within a single structure.

The routing tree is reshaped every round. As a certain number of rounds have passed, the sink will have collected information about node behaviors in different routing topologies. The information includes which nodes are bad for sure, which nodes are suspiciously bad, and the nodes' topological relationship, the sink runs heuristic ranking algorithms.

Step 1. Input is taken as tree T with each node 'a' marked by positive or negative (depending on the number of packets)
Step 2. Each leaf node 'a' in tree does perform the following functions:
a's parent is denoted as b.Since the leaf node u cannot be the sink then mark the leaf node 'a' as positive and its parent node 'b' as negative.Repeat the process until the node 'b' is a parent node.
Step 3. Mark the parent node 'b' as positive and this node is considered to be as sink.
Step 4. Since 'b' becomes sink node, assume 'a' as bad node & set a = bad node.
Step 5. Apply "PFDA (Packet Forwarding, Modifier and Droppers Attack)"method to designate the nodes a and b suspiciously either bad /good

Figure 4. PFDA Step By Step Implementation Steps

Sink Node Functions

- Verify - Sink receives all packets from the sender node, and it verifies all packets which are dropped or not. And it also verifies the packets which are modified or not and it can identify the modifiers in the process based on the bit identification.
- Merge Packets- After receiving all packets in sink, it decrypts all packets. After the decryption if there is no modified or dropped packets, it merge all packets. After merging, Sink can receive the original file.
- Categorization and Ranking- In this Categorization and Ranking will be performed based on the node behavior. If there is any modification or drop of packets in node it assumes negative value for modifier or dropper.

Heuristic Ranking Algorithm is based on the number of times a node is identified as suspiciously bad then that node is considered as a most likely bad node. [3]Thus to study the behavior of a node, it is assumed that nodes continuously monitor the forwarding behaviors of their neighboring nodes to determine if their behavior is anomalous.

IV. Results & Discussion

Network configuration is done with n number of nodes where n is assumed. Figure.13. shows the output of network configuration as implemented in Java. In this network configuration, creation of network is achieved by connecting n number of nodes. By using frames concept in java, the nodes are created. The network group is categorized in various levels that depend on number of nodes. Here three levels are implemented. Figure 6 and 7 shows the node configuration at levels 0 and 1 . In level 1, the network group is created by connecting node 1 at level 0 to sink node at level 1. Socket programming concept is implemented for connection of the two nodes. Similarly nodes are configured in further levels. Frames concept is embedded in this node configuration. Now the hierarchical tree is plotted. Next step is to consider an input file and send it across the root node which becomes the source of transmission which is shown in figure 8.

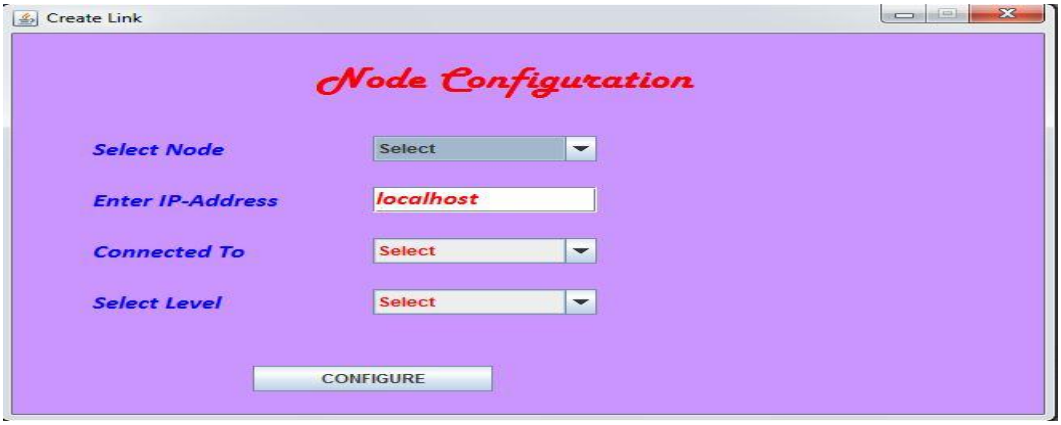


Figure 5. Node configuration at level 1

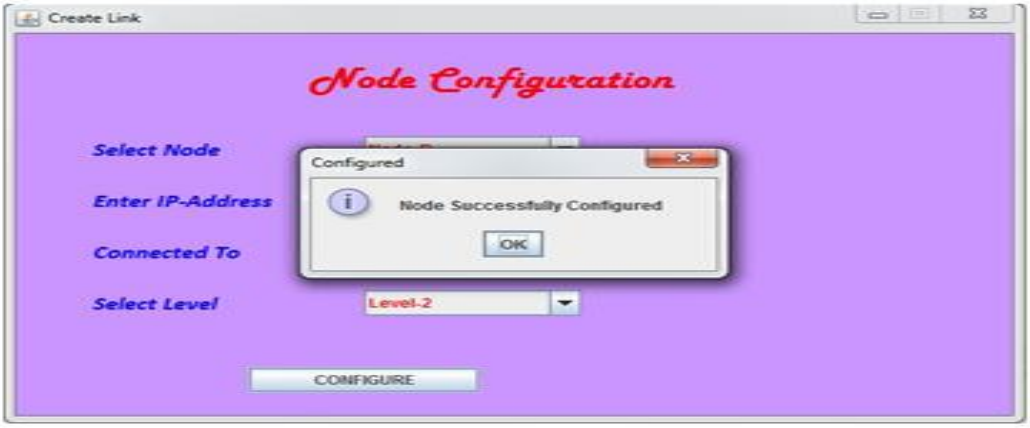


Figure6. Node level 0

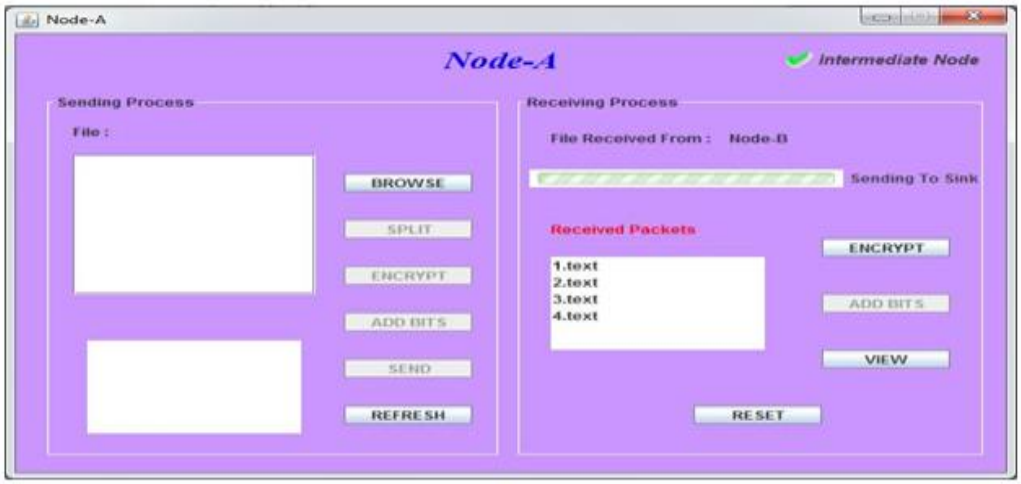


Figure 7. Sender Node Sending The Input To Sink

Figure 9. Sender Node Splitting Into Packets & Then Apply Encryption

Figure 9 shows sending packets from intermediate node that is node A to sink node.Bits are added to the packets after splitting and encrypting the data for source node identification. It means to identify that from which node, the data is forwarded. Now the the packets are forwarded to intermediate nodewithout being dropped. Therefore this task is completed after adding bits to the packets at intermediate node.

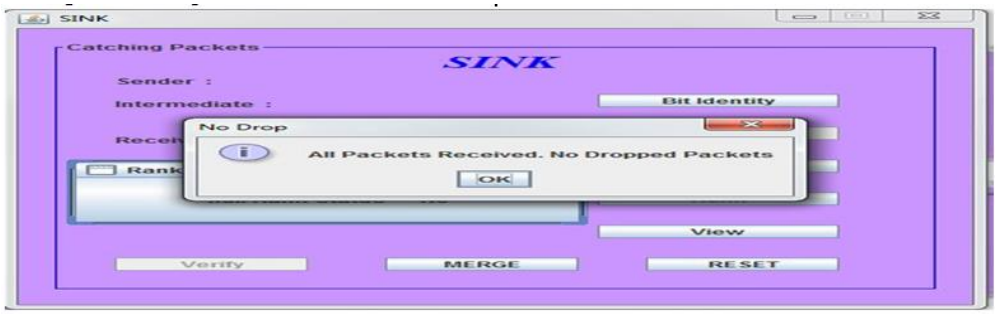


Figure 10.Receiver node receiving the packets at sink node

Figure 10 show that receiving packets at sink node from intermediate node after adding bits for source identification.

Figure 11.Packet Merging at sink node

Figure 11 shows after sending packets from intermediate node A to sink node then all the packets are merged to receive the original input text file. At this point the status of packet sent and received must be recorded to identify the point of packet dropping or modification.

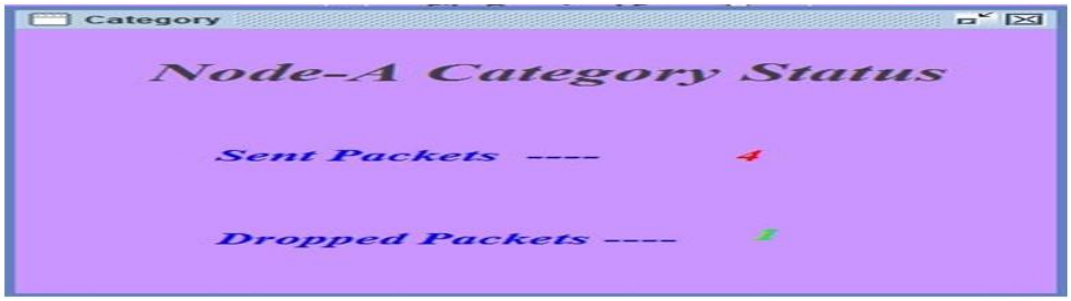
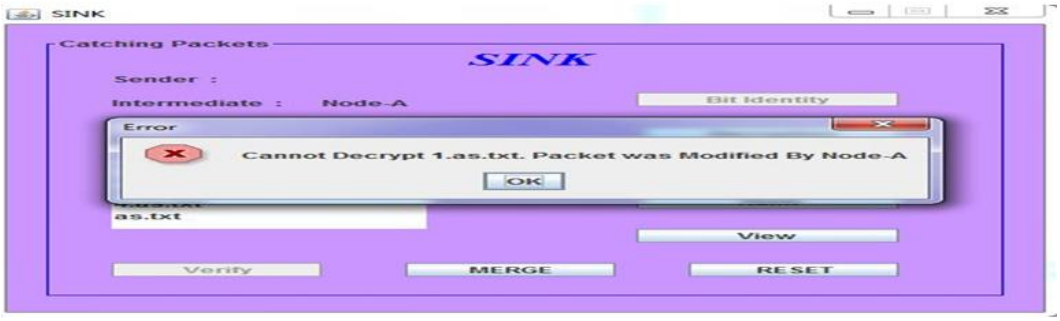
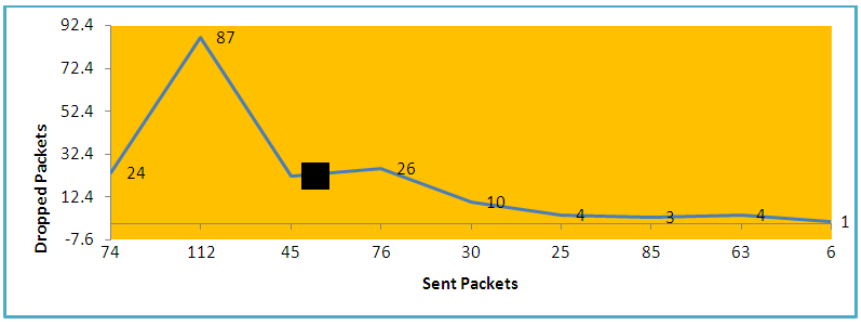


Figure 12.Packet Transmission Status

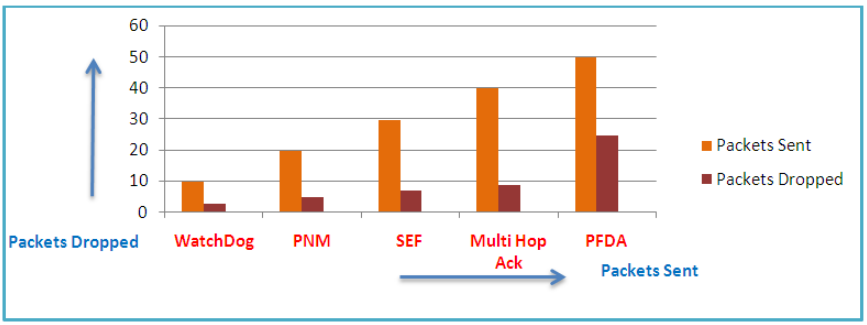
At every node, the status of packets sent vs dropped can be identified. It is observed that in figure 12, one packet is dropped from four sent packets at node A. Hence node A is identified as misbehaving node. There should be a mechanism to conclude that node A is bad. For this heuristic ranking method is applied to check whether node A is suspiciously bad or completely bad. In this context, it is assumed that if all the packets received at a given node without any dropping or modification then the node is assigned as "good" otherwise it is said to be "bad".



For instance, consider a case where a packet is being modified. This modification attack can be concluded such that if there is any deviation in the packet content before sent and while received, then such packets are difficult to receive the original content because bits added differs. Hence such packets are not easy in decryption process. Hence, which ever packets are under such analogy, then it is said that packet modify attack has taken place. Figure 13 shows that the packets are modified at node A. This is identified and node A is thus again concluded as misbehaving node.UsingQiMacros tool, the traffic simulation is plotted from a manet with appropriate ratio of packets sent & dropped.



This graph depicts the sent packets and the percentage of dropped packets. It conveys that when 74 packets are sent, 24 packets are found as dropped (32%). Similarly, when 112 packets are sent, 84 packets were dropped (75%).



The proposed model is checked with existing system. The average accuracy values for proposed system, Multi Hop Ack, PNM and watchdog are 25%,9%,7%,5% and 3% respectively. Thus the motive of providing a better technique to catch dropped packets is achieved.

V. Conclusion

An effective scheme called as "PFDA (packet forwarding, modifier and droppers attack)" is used to detect three types of attackers, as packet forwarders, modifiers & packet droppers. It is implemented with a hierarchical structure by establishing a routing tree. The scheme is focused towards behavioral study of the

nodes in the network which are a part of the tree. The nodes behavior is monitored to identify the anomalous activity in the network. The anomalous behavior is found to be a point based rather than collective or contextual.

Modern technology implementation using My Eclipse is adopted. Hence, a single approach is proposed and was successful to detect three attackers within a single structure. The detection was found to happen at a single point, at the time of packets in transit. Packets were encrypted before transmission and still it is observed that the attackers are happened to be inside the network exploited their privileges in performing various unknown attacks. It is concluded that when packets sent is increased, the ratio of dropped packets is also increased. In this regard, the future work can be extended to study & make necessary precautions by including some prevention methods that can deal to reduce the ratio of dropped packets & increase the ratio of sent packets with adequate measures.

References

[1]. H. Chan and A. Perrig, "Security and Privacy in SensorNetworks," Computer, vol.36, no. 10, Oct. 2003.

[2]. C. Karlof and D. Wagner, "Secure Routing in Wireless SensorNetworks: Attacks andcountermeasures," Proc. IEEE First Int'lWorkshop Sensor Network Protocolsapplications03Applications, 2003.

[3]. V. Bhuse, A. Gupta, and L. Lilien, "DPDSN: Detection of Packet-Dropping Attacksforwireless Sensor Networks," Proc. FourthTrusted Internet Workshop, 2005.

[4]. M. Kefayati, H.R. Rabiee, S.G. Miremadi, and A. Khonsari, "Misbehavior Resilient Multi Path Data Transmission in MobileAd-Hoc Networks," Proc. Fourth ACM Workshop sec urity of Ad Hoc and Sensor Networks 2006.

[5]. R. Mavropodi, P. Kotzanikolaou, and C. Douligeris, "Secmr—ASecure MultipathRouting Protocol for Ad Hoc Networks," Ad HocNetworks, vol. 5, no. 1, pp. 87-99,2007.

[6]. F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical En-Route Filteringof Injected FalseData inSensor Networks," Proc. IEEE INFOCOM,2004.

[7]. S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An Interleaved Hop-by-Hop Authentication schemScheme for Filtering False Data in SensorNetworks," Proc. IEEE Symp. Security 2004.

[8]. H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, "TowardResilient Security inWireless se-nsor Networks," Proc. Sixth ACMInt'lSymp. Mobile Ad Hoc Networking 2005.

[9]. S. Lee and Y. Choi, "A Resilient Packet-Forwarding Scheme Against MaliciouslyPacket-Dropping Nodes in Sensor Net-works," Proc. Fourth ACM Workshop onSecurity of Ad Hoc and Sensor Networks (SASN '06), 2006.

[10]. I. Khalil and S. Bagchi, "MISPAR: Mitigating Stealthy Packet Dropping in Locally-Monitored Multi-Hop Wireless Ad Hoc Networks," Proc. Fourth Int'l Conf.Security and Privacy in Comm. Netowrks (SecureComm '08), 2008.

[11]. I. Krontiris, T. Giannetsos, and T. Dimitriou, "LIDeA: A Distributed LightweightIntrusion Detection Architecture for Sensor Networks," Proc. Fourth Int'l Conf.Security and Privacy in Comm. Netowrks (SecureComm '08), 2008.

[12]. S. Ganeriwal, L.K. Balzano, and M.B. Srivastava, "Reputation-Based Framework for High Integrity Sensor Networks," ACM Trans. Sensor Networks, vol. 4, no. 3, pp. 1-37, 2008.

[13]. W. Li, A. Joshi, and T. Finin, "Coping with Node Misbehaviors in Ad HocNetworks: A Multi-Dimensional Trust Management Approach," Proc. 11th Int'l Conf. Mobile Data Management (MDM '10), 2010. P. Michiardi and R. Molva, "Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks," Proc. IFIP TC6/TC11 Sixth Joint Working Conf. Comm. and Multimedia Security: Advanced Comm. and Multimedia Security,

[14]. S. Buchegger and J. Le Boudec, "Performance Analysis of the Confidant Protocol,"Proc. ACM MobiHoc, 2002.

[15]. F. Ye, H. Yang, and Z. Liu, "Catching Moles in Sensor Networks,"Proc. 27th Int'l Conf. Distributed Computing Systems (ICDCS '07),2007.