MISBEHAVIOUR DETECTION AND ISOLATION SYSTEM IN WIRELESS ADHOC NETWORKS

Atul Kumar A[1], Ashwin Raj S N[2], Ashok P[3]

[1] *Department of Electronics and Communication Engineering, Prince Shri Venkateshwara Padmavathy Engineering College, Chennai, India*
[2] *Department of Electronics and Communication Engineering, Prince Shri Venkateshwara Padmavathy Engineering College, Chennai, India*
[3], *Assistant Professor, Department of Electronics and Communication Engineering, Prince Shri Venkateshwara Padmavathy Engineering College, Chennai, India*

ABSTRACT

In general the misbehaving nodes in a wireless networks can only be identified but cannot be isolated. In this paper, we propose a architecture namely misbehaviour detection and isolation system in wireless networks by using AODV(Ad-hoc On Demand Distance Vector) algorithm. This is a technique used to support maximum number of nodes and maintaining a clear view of all the nodes present in the corresponding network. This system combines the Cluster based(CB) and the acknowledgement based systems. The results are in such a manner that Packet delivery ratio is increased and the isolation of misbehaviour nodes is performed.

Keyword: - *Misbehaviour nodes, Audit based detection, AODV detection techniques*

1. INTRODUCTION

This project closely investigates a comprehensive system called Misbehaviour Detection and Isolation System that effectively and efficiently isolates both continuous and selective packet droppers. The system integrates reputation management, trustworthy route discovery, and identification of misbehaving nodes based on behavioral audits.Ad hoc networking describes a mode of connecting electronic devices to one another without the use of a central device like a router that conducts the flow of communications.

Devices connected to an ad-hoc network, called nodes, each forward data to other nodes.In the existing system, a particular amount of misbehaviouring nodes may occur in the path of different networks. So, these misbehaviouring nodes may be identified in the path, but they cannot be isolated from the remaining networks.Routing like BFTR has been used to detect such misbehaviour nodes.The main drawbacks in the conventional system are that packet delivery ratio has been much affected and Illegal access of data has been prevailing.

2. PROPOSED SYSTEM

Misbehaviour Detection And Isolation System in Wireless Adhoc Networks, which achieves per-packet behavior evaluation without incurring a per-packet per-hop cost. It is a comprehensive solution that integrates identification of misbehaving nodes, reputation management, and trustworthy route discovery in a distributed and resource-efficient manner. In our work we adopt a system that satisfies the homomorphic multiplication property such as RSA. The development of a key management system for establishing trust within the network is beyond the scope of the present work. It also provides a comprehensive misbehavior identification and node isolation system for eliminating misbehavior from a given network. This system consists of the integration of three modules: a reputation module, a route discovery module, and an audit module.

The Most important characteristics of the wireless networks is the Mobile Ad Hoc Networks and the most important feature is that all the devices can act as both transmitter and receiver also MANETs are used in various fields like military, industry emergency recovery. But there is a certain faults in the system, such that there are drawbacks in MANETs, that it becomes prone to malicious attacks very fast. To avoid such attacks a good intrusion detection and prevention system is needed. In this paper, we proposed a system which can detect as well as prevent the malicious attacks.

2.1 Network Formation

Wireless ad-hoc networks realize end-to-end communications in a cooperative manner. Nodes rely on the establishment of multi-hop routes to overcome the limitations of their finite communication range this paradigm, intermediate nodes are responsible for relaying packets from the source to the destination. As a source S using a multi-hop path to route data to a destination D.

This network model presupposes that intermediate nodes are willing to carry traffic other than their own. When ad-hoc networks are deployed in hostile environments (tactical networks), or consist of nodes that belong to multiple independent entities, a protocol-compliant behavior cannot be assumed. Unattended devices can become compromised and drop transit traffic in order to degrade the network performance. Figure 3.1 refers represents the flow diagram for network formation.

2.2 Modules

- Cooperation Incentive-based Approaches
- Audit-based Misbehavior Detection (AMD)
- Intrusion Detection System (IDS)

2.2.1 Cooperation Incentive Based Approaches

The Previous methods for eliminating packet droppers can be classified into (a)credit-based systems (b)reputation-based systems and (c)acknowledgment-based systems. Credit-based systems are designed to provide incentives for forwarding packets. While credit-based systems motivate selfish nodes to cooperate, they provide no incentive to malicious nodes.

Such nodes have no intend to collect credit for forwarding their own traffic. Reputation-based systems use ratings for evaluating the trustworthiness of nodes in forwarding traffic.It use neighboring monitoring techniques to evaluate the behavior of nodes. These scheme which relies on two modules, the watchdog and the path rater Acknowledgment-based systems.

They rely on the reception of acknowledgments to verify that a message was forwarded to the next hop ACK-based systems also incur a high communication and energy overhead for behavioral monitoring they cannot detect attacks of selective nature over encrypted end-to-end flows. Figure 3.2 represents the corresponding flow diagram for Co-operative Incentive Based Approach.

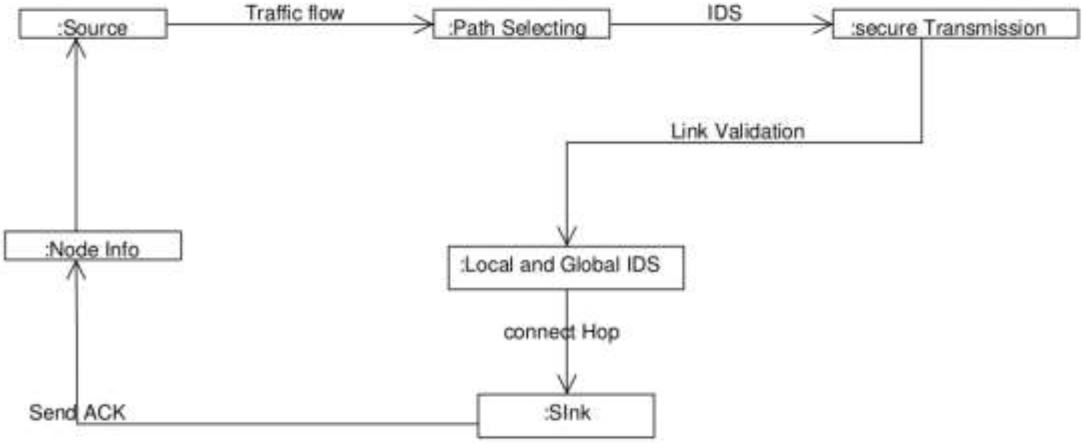


Figure 2.1 Flow diagram for Co-operative Incentive Based Approach

In the figure 2.1, initially the source will be responsible for selection of path for its data transmission. Using Intrusion Detection System (IDS), the secured transmission of packets is established. The link between the source and the destination will be validated based on the incentives. Depending upon their range whether it is local or global, the nodes which have lower incentives/trust values will be excluded.

2.2.2 a) Credit Based Systems

Credit based systems are such that they provide incentives for forwarding packets. Buttyan and Hubaux proposed a system in which nodes accumulate credit for every packet they forward, and spend their credit to transmit their own packets. To ensure correctness, the credit counter is implemented in tamper-proof hardware.

While credit-based systems motivate selfish nodes to cooperate, they provide no incentive to malicious nodes. Such nodes have no intend to collect credit for forwarding their own traffic. Moreover, credit- based systems do not identify misbehaving nodes, thus allowing them to remain within the network indefinitely.

2.2.2 b) Reputation Based Systems

Reputation-based systems use ratings for evaluating the trustworthiness of nodes in forwarding traffic. These ratings are dynamically adjusted based on the nodes' observed behavior. In the context of ad hoc networks, Ganeriwal and Srivastava developed a Bayesian model to map binary ratings to reputation metrics, using a beta probability density function.

Reputation-based systems use neighboring monitoring techniques to evaluate the behavior of nodes. Marti proposed a scheme which relies on two modules, the watchdog and the path rater . The watchdog module is responsible for overhearing the transmission of a successor node, thus verifying the successful packet forwarding to the next hop. The path rater module uses the accusations generated by the watchdog module to select paths free of misbehaving nodes.

When misbehavior is detected, monitoring nodes broadcast alarm messages in order to notify their peers of the detected misbehavior and adjust the corresponding reputation values. Similar monitoring techniques have also been used in transmission overhearing becomes highly complex in multi-channel networks or when nodes are equipped with directional antennas. Neighboring nodes may be engaged in parallel transmissions in orthogonal channels or different sectors thus being unable to monitor their peers. Moreover, operating radios in promiscuous mode for the purpose of overhearing requires up to 0.5 times the amount of energy for transmitting a message . Note that for a multi-hop route, a given packet must be overheard by multiple monitors and over multiple hops, thus making the monitoring operation more expensive than the actual end-to-end communication.

Finally, neighboring monitoring typically record coarse metrics of misbehavior such as packet counts that are inadequate to detect highly sophisticated selective dropping attacks tailored to specific applications. Motivated by the inadequacy and inefficiency of transmission overhearing, the monitoring approach developed in AMD incurs overhead on a per-flow basis instead of on a per-packet basis, thus having significantly smaller energy expenditure. Moreover, it allows the full customization of the misbehavior criteria for detecting a multitude of selective dropping strategies.

2.2.2 c) Acknowledgement Based Systems

Acknowledgment-based systems rely on the reception of acknowledgments to verify that a message was forwarded to the next hop. A scheme called TWOACK, where nodes explicitly send two-hop acknowledgment messages along the reverse path, verifying that the intermediate node faith- fully forwarded packets. Packets that have not yet been acknowledged remain in a cache until they expire. A value is assigned to the quantity/frequency of un-verified packets to determine misbehavior. Liu improved on TWOACK by proposing 2ACK. Similar to TWOACK, nodes explicitly send two-hop acknowledgments to verify cooperation. The source probes intermediate nodes to acknowledge each packet and performs a binary search to identify the link where packets are dropped.

ACK-based systems also incur a high communication and energy overhead for behavioral monitoring. For each packet transmitted by the source, several acknowledgements must be transmitted and received over several hops. Moreover, they cannot detect attacks of selective nature over encrypted end-to-end flows.

2.2.2 Audit Based Misbehaviour Detection (AMD)

In the absence of a supporting infrastructure, wireless adhoc networks realize end-to-end communications in a cooperative manner. Nodes rely on the establishment of multi-hop routes to overcome the limitations of their finite communication range. In this paradigm, intermediate nodes are responsible for relaying packets from the source to the destination.This network model presupposes that intermediate nodes are willing to carry traffic other than their own. When ad hoc networks are deployed in hostile environments (tactical networks), or consist of nodes that belong to multiple independent entities, a protocol-compliant behavior cannot be assumed. Unattended devices can become compromised and drop transit traffic in order to degrade the network performance. Moreover, selfish users may misconfigure their devices to refuse forwarding traffic in order to conserve energy. This type of behavior is typically termed as node misbehavior.

The AMD system is developed for detecting and isolating misbehaving nodes. Compared to state-of-the-art, AMD provides the following additional features. AMD enables the per-packet evaluation of a node’s behavior without incurring a per-packet overhead. AMD enables the concurrent first-hand evaluation of the behavior of several nodes that are not necessarily one-hop neighbors. Overhearing techniques are limited to one hop. AMD can operate in multi-channel networks and in networks with directional antennas. Current packet overhearing techniques are only applicable when transmissions can be overhead by peers operating on the same frequency band.AMD detects selective dropping behaviors by allowing the source to perform matching against any desired selective dropping patterns. This is particularly important when end-to-end traffic is encrypted. In the latter scenario, only the source and destination have access to the contents of the packets and can detect selective dropping. The AMD can construct paths consisting of highly trusted nodes, subject to a desired path length constraint.

2.2.3 Incremental Intrusion Detection System (IDS)

An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Any detected activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system combines outputs from multiple sources, and uses alarm filtering techniques to distinguish malicious activity from false alarms. There is a wide spectrum of IDS, varying from antivirus software to hierarchical systems that monitor the traffic of an entire backbone network. The most common classifications are network intrusion detection systems (NIDS) and host-based intrusion detection systems (HIDS). A system that monitors important operating system files is an example of a HIDS, while a system that analyzes incoming network traffic is an example of a NIDS. It is also possible to classify IDS by detection approach: the most well-known variants are signature-based detection (recognizing bad patterns, such as malware) and anomaly-based detection (detecting deviations from a model of "good" traffic, which often relies on machine learning). Some IDS have the ability to respond to detected intrusions. Systems with response capabilities are typically referred to as an intrusion prevention system.

2.3 Block diagram

The block diagram shown in figure 2.2 is for the appointment of a cluster head and making it lookout for all the misbehaviour nodes that are present in the network. The appointment of the cluster head is done depending upon the Number of energy levels among different nodes thereby providing a safe and secure path and not sending any data through the misbehaviouring node again.

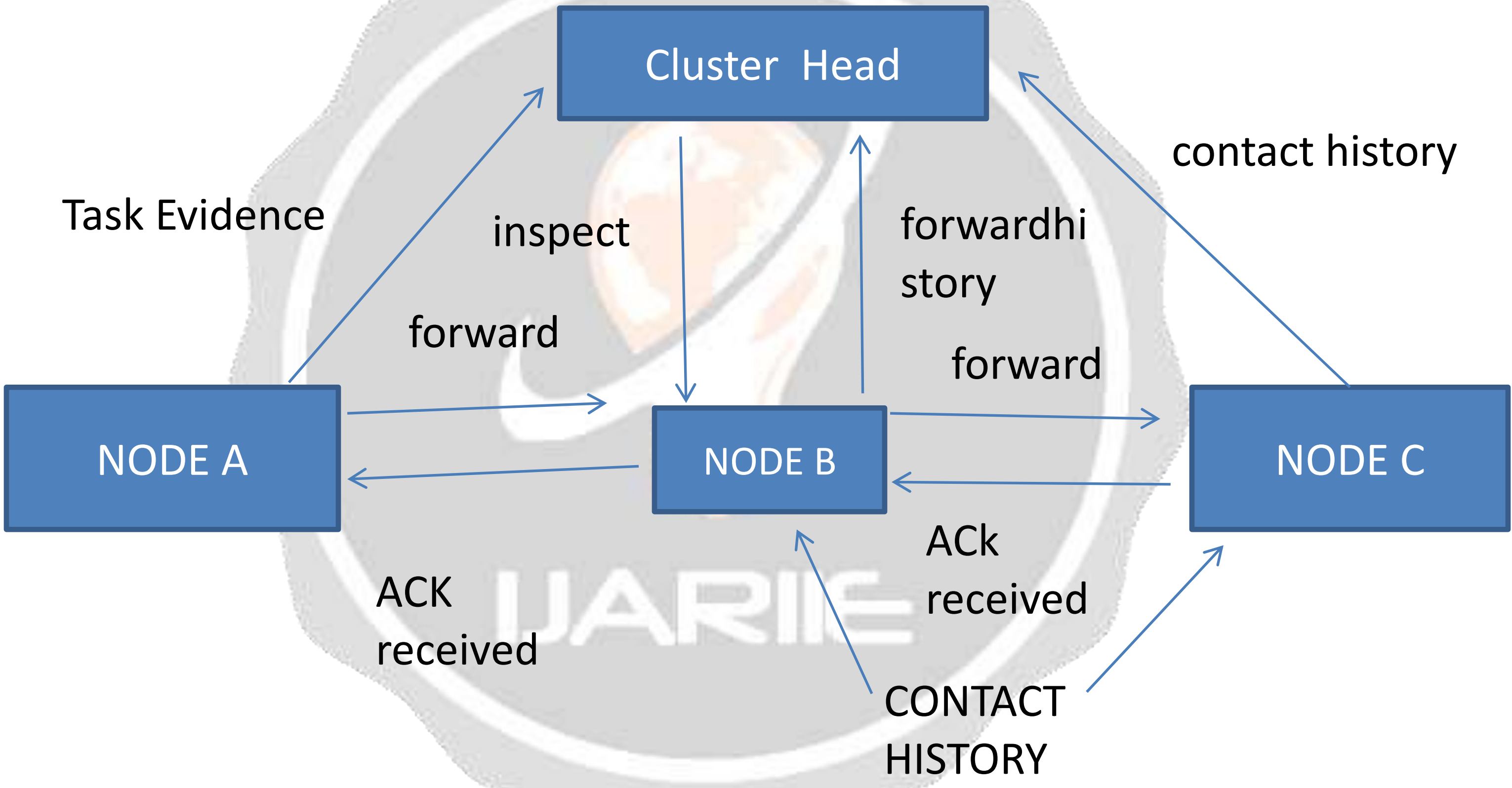


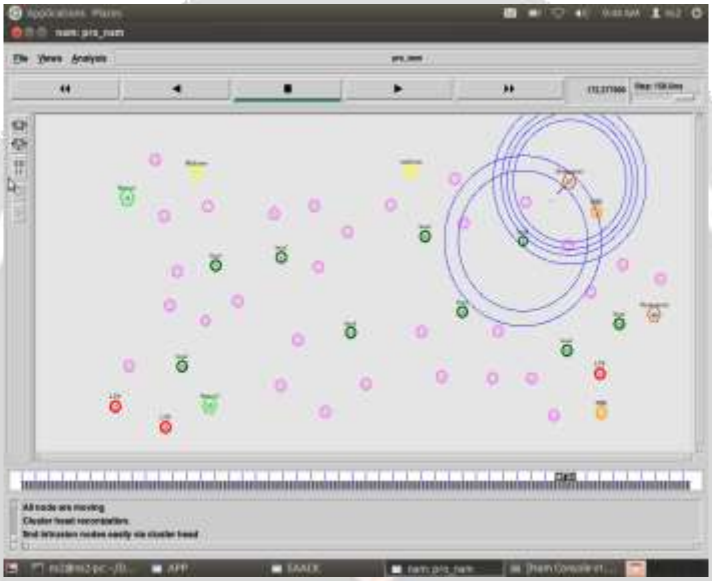
Figure 2.2 Block diagram of Proposed System

3. RESULTS AND DISCUSSIONS

The following set of nodes will be present and the source and the destination will be selected initially. So, a packet from the source node will be delivering a packet to the next node such that the path will be chosen randomly. So , In order to obtain the acknowledgement from the destination, AACK scheme will be used where the acknowledgement will be made by one on one hop.The next path will be chosen such that if a misbehaviour node is identified the packet drop will happen and some node in its path will be identified as LTP, suh that the amount of power used in this node will be less when compared to the other nodes.The nodes that sends a false misbehaviour report to the previous node will be identified and the packet drop occurs. So, the detection process is performed and follows the isolation process is continued.

Same initial packet delivery is made and the acknowledgment is made by both AACK and 2-ACK Scheme, where 2-ACK scheme allows the acknowledgement to be made for 2 hops before the present node.Whenever nodes are reported as misbehaviour, then a MRA node will be identified such that the MRA will keep an account of that misbehaviouring node and it wont send any packets or acknowledgement through that misbehavioring node.Finally these set of nodes will be divided in the form of clusters such that the misbehaviouring nodes will be identified easily and the best path will be chosen at random. So, this concludes with the fact that misbehaviouring nodes are both detected and isolated.

Figure 3.1 shows the overall performance and packet delivery to the destination nodes including all the factors that affect the packet transmission and sends the packets successfully.



All node are moving
Cluster head reconstation
find intrusion nodes easily via cluster head

Figure 3.1 Packet delivery to the destination nodes

.

4. REFERENCES

[1].G. Acs, L. Buttyan, and L. Dora, “Misbehaving router detection in link-state routing for wireless mesh networks,” inProc. IEEE Int.Symp. World Wireless Mobile Multimedia Netw., 2010, pp. 1–6

[2]. K. Balakrishnan, J. Deng, and P. K. Varshney, “Twoack: Preventing selfishness in mobile Ad Hoc networks,” in Proc. IEEE Wireless Commun. Netw. Conf., 2005, pp. 2137–2142.

[3]. L. Buttyan and J.-P. Hubaux, “Stimulating cooperation in self-organizing mobile Ad Hoc networks,”Mobile Netw. Appl., vol. 8,no. 5, pp. 579–592, 2003.

[4]. M. Hietalahti, “A clustering-based group key agreement protocol for ad-hoc networks”. Electronic Notes in Theoretical Computer Science, Vol.192,pp.43-53, 2008.