Audit based Misbehaviour and Gray-hole detection in spontaneous wireless Adhoc network

Nafees Muneera.M, Thirupurasundari.D.R

Abstract: Spontaneous Adhoc network are formed by a set of mobile terminals placed in a close location that communicates with each other, share resources, services or computing time during a limited period of time and in a limited space. In the proposed system, the process of creating spontaneous wireless adhoc network, identifying gray hole attack in the system, detecting misbehaviour of the nodes by audit based misbehaviour detection system and increase in security have been discussed. To enhance the security, the group key is generated and distributed among the nodes. Gray hole is a malicious attack that makes the node to refuse forwarding certain packets and to drop the packet. The attacker selectively drops the packets originating from a single IP address or a range of IP addresses and forwards the remaining packets. It is detected and rectified using the Sequenced Queue based Routing Algorithm (SQRA).

***Misbehaviour of the nodes is detected using Audit based misbehavior detection system (AMD). It has a reputation module, route discovery module and an audit module. The reputation module is responsible for managing reputation information based on the recommendations of the audit module. The reputation values are exploited by the route discovery module for establishing routes that exclude nodes with low reputations. Finally, the audit module efficiently identifies the misbehaving nodes via an audit process*.**

Keywords – **Adhoc network, spontaneous network, Misbehavior, Reputation system.**

---

1. INTRODUCTION

Communication being a mode of sending and receiving information is gaining more popularity in today's world. There are various modes of communication; one is wireless mode; in which communication takes place through an open medium. Wireless 802.11 networks can be categorized in to two types: Infrastructure mode and Adhoc mode.

- ***Nafees Muneera.M*** *is currently pursuing Masters Degree program in Computer Science and Engineering. Ph.9840332760*
- ***Thirupurasundari.D.R****, M.E., Asst.Prof., Dept of Computer Science and Engineering, Ph-9840883458*

Infrastructure mode has a fixed backbone for communicating with each other. An Ad-hoc network is the collection of nodes which can communicate with each other without any infrastructure .Wireless medium is a medium which can be accessed by both legitimate users and attackers. To detect audit based misbehaviour and gray -hole intrusion in Spontaneous wireless ad-hoc network to enhance the security for node connectivity.

The proposed system is based on the concept of spontaneous wireless ad-hoc network. It is created by a master laptop with various nodes that falls into the range. The scope of the proposed system is to introduce enhanced network security to avoid re-connecting/accessing of the network by the nodes that are withdrawn from the network before expiry of their session. This is achieved by adopting "Gray Hole Intrusion" in spontaneous wireless ad-hoc network. Along with this the misbehavior of the other nodes are also detected using the "audit based misbehavior detection system" during transactions.

1.1 Wireless Network

Wireless network technologies come in several forms such as wireless PAN, Wireless LAN and Wireless WAN. These networks have their own characteristics and properties. Wireless PANs are those networks in which the interconnected devices communicate using either Zig Bee or Bluetooth. The range of this communication is very less, say 10m.Wireless LANs are networks that have various devices capable of communicating with each other.

1.2 Adhoc- Network

An ad-hoc network can be formed when a group of mobile devices communicate with each other without depending on any fixed infrastructure. In such cases, neighbouring nodes communicate with each other while the communication between non-neighbour nodes is performed via the intermediate nodes that can act as routers. The network topology frequently changes in the adhoc network. Ad-hoc wireless network are prone to route breaks due to various sources such as node mobility, signal interference, high error rate and packet collision.

An adhoc network among three laptops and the boundary is defined among them and is shown in the below Fig.1.1.

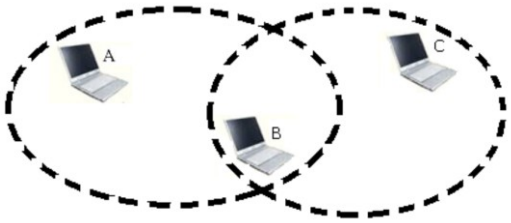

Fig.1.1 Adhoc network

1.3 Routing in Adhoc Network

Routing in an adhoc network is the most important task that needs to be handled with care. Since the nodes in an adhoc network depend on intermediate nodes, for carrying the data there are various routing protocols used in this process. The main aim of routing protocols in an adhoc network is to find minimum hop distance between the source and destination with minimum overhead and bandwidth. Depending on the routing topology, they are classified as proactive, reactive and hybrid.

In the proposed system, a reactive protocol namely Dynamic Source Routing (DSR) is used. Dynamic Source Routing is a reactive routing protocol which is able to handle the dynamically changing topology. It is also called as source routing because each data packet should traverse to reach destination. It also operates on two steps: Route Discovery and Route maintenance. Source node uses route discovery process to find the path to destination. It also uses control messages such as RREQ, RREP. The process of route discovery and route reply is given in the below Fig.1.2.

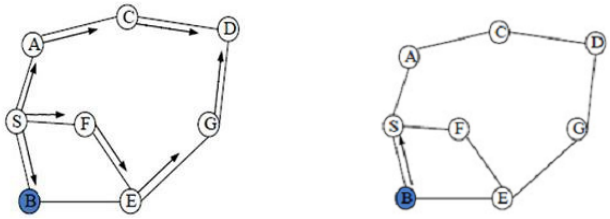

Fig.1.2 Route discovery and route reply

2. RELATED WORK

2.1 Spontaneous Wireless Adhoc Network Creation

In this paper, a secure protocol has been proposed for spontaneous wireless adhoc networks. This uses a hybrid symmetric/asymmetric scheme and the trust between users in order to exchange the initial data and to exchange the secret keys that will be used to encrypt the data. Trust is based on the first visual contact between the users. This is a complete self – configured secure protocol that is able to create the network and share secure services without any infrastructure. The network allows sharing of resources and offers new services among users in a secure environment. Co-operation between devices allows provision and access to different services, such as group communication, collaboration in program delivery, security. Each node must configure its own data: IP, port data security, and user data. The network members and services may vary because devices are free to join or leave the network. Memory consumed in each operation during Spontaneous Network Creation is high. This paper provides some procedures for self configuration: a unique IP address is assigned to each device, the DNS can be managed efficiently and the services can be discovered automatically.

2.2 Gray Hole Attack

MANET is one of the most important technologies that have gained interest due to recent advantages in both hardware and software techniques. Manet technology allows a set of mobile users equipped with radio interfaces to discover each other dynamically from a communication network. Manet incorporates routing functionality into mobile nodes and thus effectively become the infrastructure. This provides multiple routing paths between any source and destination. Gray hole attack is a malicious node that refuses to forward certain packets and simply drops them. The attacker selectively drops the packets originating from a single IP address or a range of IP addresses and forwards the remaining packets. Gray hole nodes in Manets are effective. Every node maintains a routing table that stores the next hop node information for a route a packet to destination node. When a source node wants to route a packet to the destination node, it uses a specific route if such a route is available in its routing table. Otherwise, nodes initiate a route discovery process by broadcasting Route Request (RREQ) message to its neighbours. On receiving RREQ message, the intermediate nodes update their routing tables for a reverse route to source node. A Route Reply (RREP) message is sent back to the source node when the RREQ query reaches either the destination node itself or any other node that has a current route to destination.

2.3 AMD: Audit Based Misbehavior Detection

In this paper, the problem of identifying and isolating misbehaving nodes that refuse to forward packets in multi-hop adhoc networks is used here. A comprehensive system called Audit Based Misbehaviour Detection (AMD) that effectively and efficiently isolates both continuous and selective packet droppers. The AMD system integrates reputation management, route discovery and identification

of misbehaving nodes based on behavioural audits. AMD evaluates node behaviour on per packet basis, without employing energy expensive overhearing techniques or intensive acknowledgement schemes. AMD can detect selective dropping attacks even if end-to-end traffic is encrypted and can be applied to multi-channel networks or networks consisting of nodes with directional antennas. AMD avoid misbehaving nodes, even when a large portion of the network refuses to forward packets.

AMD provides the following additional features:

1. AMD enables per-packet evaluation of a node's behaviour without incurring a per-packet overhead.
2. AMD enables the concurrent first-hand evaluation of the behaviour of several nodes that are not necessarily one-hop neighbours. Overhearing techniques are limited to one hop.
3. AMD can operate in multi-channel networks and in networks with directional antennas. Current packet overhearing techniques are only applicable when transmission can be overhead by peers operating on the same frequency band.
4. AMD detects selective dropping behaviours by allowing the source to perform matching against any desired selective dropping patterns. This is particularly important when end-to-end traffic is encrypted.

2.4 Five Challenges of Spontaneous Network

An adhoc network must operate independent of a pre-established or centralized network management infrastructure, still providing administrative services needed to support applications. Address allocation, name resolution, service location, authentication and access control policies represent some of the functionality that must be supported. Spontaneous networks have a limited extent in both space and time. They comprise powerful host machines, such as laptop computers or emerging high-end personal digital assistants (PDAs) and mobile phones. The nodes are connected using a variety of wireless technologies, such as IEEE802.11, infrared(IR), or Bluetooth, meaning that bridging between heterogeneous interfaces will be an important part of multihop routing. Although the topology of a spontaneous network is unpredictable and dynamic, it is expected that significant changes will be relatively infrequent over the lifetime of the network. Wireless connectivity is based on physical proximity; it reflects the way humans interact. In particular, authentification and trust can be based on "first-person" interaction, rather than relying on centralized administrative services.Collabarative applications are intended to reflect users' interactions, making their basic structure and human-computer interface suitable for use in an adhoc environment. The notion of a spontaneous network is created when a group of people come together for some collaborative activity. Five challenges posed by spontaneous networking environment are:

1. Network boundaries are poorly defined
2. The network is not planned
3. Hosts are not preconfigured
4. There are no central servers
5. Users are not experts

2.5 Evolving Concepts and Technologies in Spontaneous network

Spontaneous networking is a means for simple integration of devices and services into networks. An over view of the evolving technologies are discussed like jini, havi and upnp. The relation of these technologies to spontaneous networking is briefed.

HAVi has been designed by eight leading vendors (Sony, Grundig,…) of consumer electronics(CEs) like TV sets, VCRs, and DVDs with the objective of easily networking them. The major design goals are exchange of control and audio/video contents, Self-configuration, Self-management, Hot plug and play, Sharing of computing and storage capacities. Universal Plug and Play (UPnP**)** Microsoft has initiated the UPnP Forum which in turn created the UPnP specification. UPnP does not invent new techniques; it uses common ones and puts them together in a framework. The design goal is to extend the known Plug-and-Play concept to a heterogeneous network environment. UPnP services are mainly WWW-based offers, and common browsers act as user interfaces.

2.6 Automatic Configuration of Ad-hoc Networks

One of the main problems when configuring ad-hoc networks is that with these networks do not have a central server with all the information of the network**.** If a new user wants to form part of a network, the user must configure his device first. A distributed protocol to network data configuration based on the use of diffusion tools and where the user's intervention is not necessary. In "Adhoc" configurations all the wireless devices must be in Adhoc mode, have the same network name (SSID), be in the same 802.11 security mode and establish the speed to which they want to transmit, this speed will be able to be established automatically. On this way, speed will be adapted in function of both the device that is connected and the quality of the sign, less the speed is, the more the sign reach will be. Each device must also have a unique IP address that identifies it on the net. This proposal is based on a distributed management of network data. A good solution to obtain high performance and improve the network

overload will be the use of MANET routing protocols that include automatic address resolution. This helps to maintain the network performance in spite of the overload that a management distributed system procedures, where nodes can have limited resources and the network can have a dynamic topology.

2.7 Adaptive Service Discovery on Spontaneous Sensor System

Natural and man-made disaster can significantly impact both people and environments. Enhanced effect can be achieved through dynamic networking of people, systems and procedures and seamless integration of them to fulfil mission objectives with service-oriented sensor systems. An Adaptive and Efficient Peer to Peer Search (AEPS) approach for dependable service integration on service-oriented architecture is based on a number of social behavior patterns. Sensor networks have the potential to revolutionize the capture, processing and communication of critical data for use of disaster rescue and relief. The functions of sensors need to be integrated to provide a joint service to meet different search and rescue requirements. Enhanced effect can be achieved through dynamic networking of people, systems and procedures and seamless integration of them to fulfill mission objectives with service oriented sensor systems. AEPS search algorithm has been evaluated for rescue capability provision. AEPS improved the scalability and performance of information and service discovery in large-scale distributed systems for the provision of dependable search and rescue capability.

3. EXISTING WORK

Spontaneous wireless adhoc networks are formed by a set of mobile terminals placed in a closed location that communicate with each other, sharing resources, services in a limited space. The integration of services and devices in the same environment enables the user to have instant service without any external infrastructure. In the spontaneous network, the first node creates the spontaneous network and generates a random session key, which will be exchanged with new nodes after the authentication phase. The architecture of the existing system is shown in the below Fig.2.1.

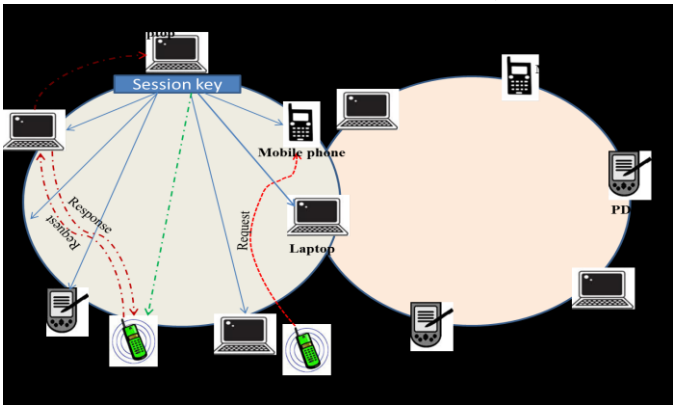

Fig 2.1 Architecture of the Existing System

The first node in the network is responsible for global settings of the spontaneous network. The second node first configures its user data and then the greeting process starts. It authenticates against the first node. Security management in the network is based on the public key infrastructure and the symmetric key encryption scheme.

3.1 Drawbacks of the Existing System

1. When a node departs from a network with a valid session key, there are possibilities for the node to perform malicious activities.
2. Intrusion detection is not detected in the system.
3. Misbehaviour of the nodes was not detected.

4. PROPOSED WORK

In the spontaneous network, the security among the nodes is enhanced by dynamic key generation. The key is generated and distributed to the nodes in the group when a transaction takes place from a source to destination. So along with the session key every node will have a group key. This avoids the entry of unauthorised node in to the transaction region. The dynamic key is generated using the ECDS algorithm.

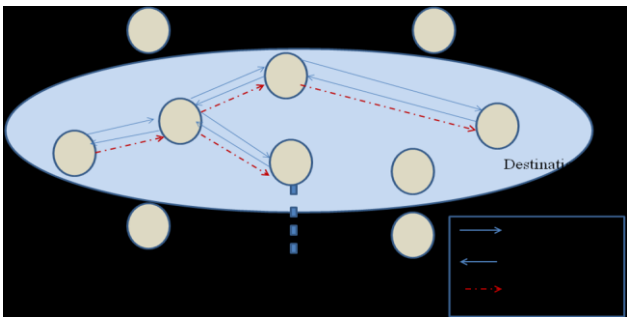

Fig 4.1 Group key generation and Gray hole detection

Gray Hole Attack is a malicious node refuses to forward certain packets and simply drops them. The attacker selectively drops the packets originating from a single IP address or a range of IP addresses and forwards the remaining packets. Gray Hole nodes in MANETs are very effective. Every node maintain a routing table that

stores the next hop node information for a route a packet to destination node , When a source node want to route a packet to the destination node , it uses a specific route if such a route is available in its routing table. Otherwise, nodes initiate a route discovery process by broadcasting Route Request (RREQ) message to its neighbours. On receiving RREQ message, the intermediate nodes update their routing tables for a reverse route to source node. A Route Reply (RREP) message is sent back to the source node when the RREQ query reaches either the destination node itself or any other node that has a current route to destination. It is detected and rectified using SQRA algorithm.

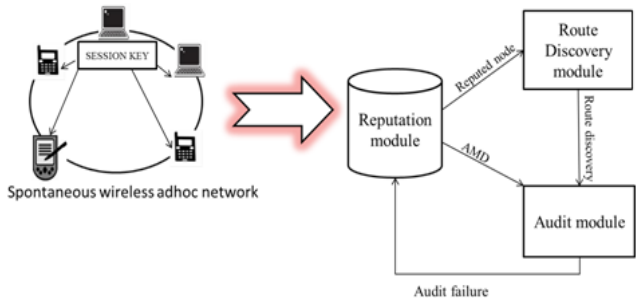

Fig.4. 2 The AMD system architecture.

This system is then inserted in to an AMD system. The AMD is the Audit based Misbehaviour detection system. AMD provides a comprehensive misbehaviour identification and node isolation system for eliminating misbehaviour from a given network. This system consists of the integration of three modules: a reputation module, a route discovery module, and an audit module. These modules closely interact to coordinate the functions of misbehaviour detection, discovery of trustworthy routes, and evaluation of the reputation of peers. A schematic of the relationship between the three modules of AMD is shown in Figure 4. 2. The reputation module is responsible for managing reputation information based on the recommendations of the audit module. Reputation values are exploited by the route discovery module for establishing routes that exclude nodes with low reputations. Finally, the audit module efficiently identifies misbehaving nodes via an audit process. This process is accelerated based on input received from the reputation module. We note that while several techniques have been proposed for reputation management and reputation-based route discovery, in AMD, we develop novel methods for these two functions that integrate efficiently with the per-flow behaviour evaluation implemented by the audit module.

5. CONCLUSION

In this paper, a spontaneous wireless Adhoc network is created, then the misbehaviour of nodes is detected and the network operations are recovered using the Audit based Misbehaviour detection system. Moreover Audit based Misbehaviour detection system can detect selective dropping attacks over end-to-end encrypted traffic streams. Thus the misbehaviour of nodes can be detected in a spontaneous wireless Adhoc network effectively.

REFERENCES

[1] J.Lloret,M.Garcia, L.Penalver," A Secure protocol for spontaneous wireless adhoc networks creation*", IEEE Transaction on parallel and distributedsystems.vol.24*

[2]Er.Shivani Sharma, Er.Tanu preet singh, "Sequenced queue based routing algorithm(SQRA) for detection and correction of gray hole attack by implementing ids*" .Proc of Intl. Conf. on Recent Trends In Computing and communication engineering.*

[3]YuZhang, Loukas zos, WilliamJr.Kozma, "AMD:Audit-based misbehavior detection in wireless adhoc networks". *IEEE transactions on mobile computing. vol.x.*

[4]L.M.Feeney, B.Ahlgren and A.Westerlund, "Spontaneous networking: an application –oriented approach to ad-hoc networking" *IEEE comm. vol39 no.6, pp.176-181*

[5]S.PreuB and C.H.Cap, "Overview of spontaneous networking – evolving concepts and technologies*",Rostocker Informatik Berichte,vol.24,pp. 113-123.*

[6]R.Lacuesta and L.Penalver,"Automatic configuration of ad-hoc networks: establishing unique ip link-local addresses*", proc.Int'l conf Emerging Security Information, systems and technology.(ICCOMP).*

[7]L.Liu,J.Xu,N.Antonopoulos, "Adaptive service discovery on service –oriented and spontaneous sensor systems*", Adhoc and sensor wireless networks, vol.4, nos.1/2,pp107-132.*

[8]Raquel Lacuesta Gilaberte, Lourdes Penalver Herrero, "IP address configuration in spontaneous networks", *Proc. Ninth WSEAS Int'l conf. Computers (ICCOMP).*

[9]Laura Marie Feeney, Bengt Ahlgren, Assar Westerlund, "Spontaneous and adhoc networks: issues and applications*" Computer and network architectures laboratory.*

[10]Ankur Bawiskar, Dr.B.B.Meshram, "Survey of attacks on wireless network" *International journal of Innovative Research in computer and communication Engineering. Vol, Issue 1.*

[1]Nafees Muneera.M has done her degree in B.E Computer Science and Engineering in C.Abdul Hakeem College Of Engineering and Technology, University of Madras, M.B.A in Operation Research from IGNOU. Now pursuing M.E Computer Science and Engineering in Meenakshi College of Engineering, Anna University, Chennai.

[2]Thirupurasundari.D.R. has done her B.Sc., degree in Computer Science in M.O.P Vaishnava College, Madras University, M.C.A from IGNOU, MPhil (Computer Science) from Periyar University, M.E (CSE) from S.M.K. Fomra Institute of Technology, Anna University. Currently, she is working as Assistant Professor in the department of Computer Science in Meenakshi College of Engineering, Anna University, Chennai.

