ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 11, May 2014

A Study on Blocking Abnormal Activities in Wireless Networks

Arvind Tudigani, Ch. Raju, Thirupathi Marupaka

Abstract *- Key applications is the routing protocol that directs the packet in the network routing packets fully connected to wireless networks has been studied to a great extent but the assumption on full connectivity is generally not valid in a real system. A class of attacks such as Network Partitioning Node Isolation attack spreads over the network are malicious pose majority threats which compromise the computer network evolve during their propagation and challenge to detect against the routing discovery. The proposed NP Hard is routing protocol blocks the abnormal activities in wireless networks when routes the packet from source to destination, the cryptography protects the message in the packet but not provides the security to the system. Comparative results on wireless network NP hard problem demonstrate the our approach interprets the system outperforms by providing the highest detection accuracy from intrusion and low false alarm rate for normal in wireless networks.*

Keywords **– Network- partitioning, Wireless Networks, Attacks, Security, Network Protocol.**

I. INTRODUCTION

Wireless LAN is important enterprise network today but end users typically do not enjoy the same level of service form wireless LAN that they come to expect from wired networks, better tools for managing wireless LAN are required for improving the quality attributes of service provided by wireless LANs. Wireless networks are fundamentally different from wired networks in that the behavior of the network is location dependent due to the nature of wireless signal propagation, the physical location of the both the transmitter and the receiver may have a large influence on the performance observed by end-users. The need for incorporating location information in wireless LAN management tools is also reflected by administrators of wireless LAN. In the access point adequate for serving the locations from where network is most actively used. Wireless networks are epicenter at its broadcast wireless network refers to any network not connected by cables which enables the desired convenience and mobility for the user. Wireless technologies use WiFi Bluetooth WiMAX as such given the diversity it is not wise to make sweeping generalizations about performance of wireless networks. Increased use of laptop computers within the enterprise increase in worker mobility have fuelled the demand for wireless networks until recently wireless technology was a patchwork of incompatible systems from a variety of vendors. Adhoc or peer-to-peer wireless network consists of a number of computers each equipped with a wireless networking interface can communicate directly with all of the wireless enabled computers they can share files and printers but may not be able to access wired LAN resource unless one of the computers acts as a bridge to the wired LAN using special software.

Wireless LAN provides network connectivity between devices also known as stations by using radio as the communication that communicate over the WLAN conform to the interfaces and procedures defined through the IEEE standards. All stations within the BSS communicate with each other through an access point in this situation the AP establishes the BSS network can consist of more than one interconnected Aps that establishes an extended service set network. Each AP within the BSS network provides 802.11 authentication services for access to the BSS network as well as privacy services for the encryption of data sent through the BSS network.

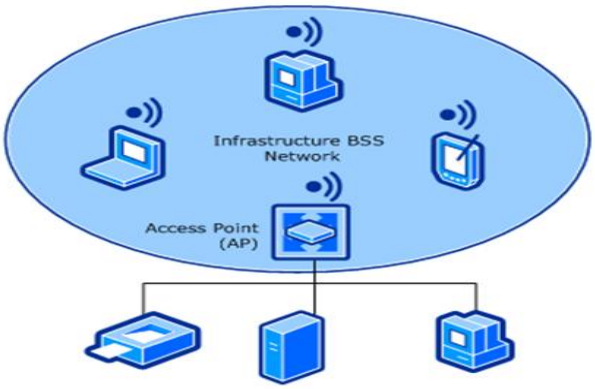

Fig 1 Location Aware Routing

In other situation topology all stations within the BSS communicate directly with each other one creates or starts the BSS network and other stations join the BSS network, which are also called as Adhoc networks provide limited support for 802.11 authentication and privacy services for the BSS network.

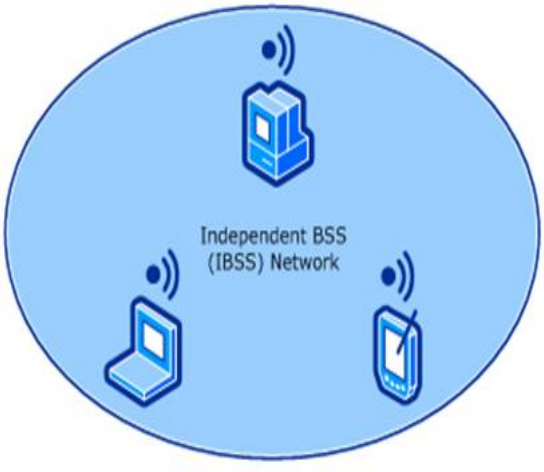

Fig 2 Location Aware Routing

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 11, May 2014

II. RELATED WORK

Quality security and privacy are important issues in any communication network have worked on these two areas as compared to MANETs and wireless sensor networks have received very attention. For client authentication andaccess control to guarantee a high-level of flexibility and transparency to all users in awireless network, the users can access the mesh network without requiring anychange in their devices and software. However, client mobility can pose severe problemsto the security architecture, especially when real-time traffic is transmitted. Tocope with this problem, proactive key distribution has been proposed.Providing security in the backbone network for WMNs is another important challenge.Mesh networks typically employ resource constrained mobile clients, which aredifficult to protect against removal, tampering, or replication. If the device can beremotely managed, a distant hacking into the device would work perfectly [7]. Accordingly, several research works have been done to investigate the use of cryptographictechniques to achieve secure communication in WMNs. In [8], security architecturehas proposed that is suitable for multi-hop WMNs employing PANA (Protocolfor carrying Authentication for Network Access) [9]. In the scheme, the wirelessclients are authenticated on production of the cryptographic credentials necessary tocreate an encrypted tunnel with the remote access router to which they are associated.Even though such framework protects the confidentiality of the information exchanged,it cannot prevent adversaries to perform active attacks against the networkitself. For instance, a malicious adversary can replicate, modify and forge the topologyinformation exchanged among mesh devices, in order to launch a denial of serviceattack. Moreover, PANA necessitates the existence of IP addresses in all the meshnodes, which is poses a serious constraint on deployment of this protocol.Authenticating transmitted data packets is an approach for preventing unauthorizednodes to access the resources of a WMN. A light-weight hop-by-hop access protocol (LHAP) has been proposed for authenticating mobile clients in wireless dynamic environments, preventing resource consumption attacks [10]. LHAP implements lightweighthop-by-hop authentication, where intermediate nodes authenticate all the packetsthey receive before forwarding them. LHAP employs a packet authentication techniquebased on the use of one-way hash chains. Moreover, LHAP uses TESLA [11] protocol to reduce the number of public key operations for bootstrapping and maintaining trust between nodes.

III. TYPES OF ROUTING

A. *Multipath Routing*

Multipath routing protocols for wireless networks areunipath means only single route is used between a source and destination node. Multipath routing is to allow the use of several good paths to reach destinations achieved without imposing excessive control overhead in maintaining multiple paths between a source and a destination.

Redundancy in the network or providing backup routes to be used when there is a failure are forms of introducing fault tolerance at the routing level in wireless networks which consists in modifying the route of a packet if the actual route broken. Bandwidth routing along single path may not provide enough bandwidth for a connection using simultaneously multiple paths to route data can be good approach to satisfy the bandwidth requirement of some applications.Suppose traffic distribution is not equal in all links in the network spreading the traffic along multiple resources can alleviate congestion in some links. Multipath protocols can be used to provide error resilience by distributing traffic over multiple paths, security routing protocols is easy for an adversary to launch routing attacks but multipath offers attack resilience.

B. *Protocol*

Protocol defines rules and conventions for communication between network devices for computer networking all generally use packet switching techniques to send and receive messages in the form packets include mechanisms for devices to identify and make connections with each other as well formatting rules that specify how data is packaged into messages sent and received.

Uses of network sharing and transferring files within networks are very rapid while maintaining integrity of the file. Individually licensed copies of many popular software programs can be costly shared programs on a network version allows for easier upgrading of the program on one single file server instead of upgrading individual workstation. Sensitive files and programs on a network are passwords protected as copy inhibit. Software can be loaded on one computer eliminating that need to spend time and energy installing updates and tracking files on independent computers throughout the building. E-mail aids in personal and professional communication electronic mail on a LAN can enable staff to communicate within the building.

C. *Selection of Route*

To develop multipath routes nodes execute a special designed route which results path are guaranteed not to interface with each other and path is executed whenever path disrupted. Operation of the reactive component of the protocol is described the requirements protocol needs to accomplish its characteristics, the first and last nodes of the path all have to be in the range of the sender receiver which means that first and last hops of the path and no link is used in two different location of paths means node disjoint and link disjoint at the same time. To reduce the overhead the multipath routing protocol maintained in each node for each route should be minimal, each node maintain a link state database of the

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 11, May 2014

overlay defined by the cluster heads that result from the clustering. Cluster heads do not interfere with each in the worst case nodes will be needed to link two cluster heads so that the information forms the topology table and refers to the cluster head nodes and the gateway nodes that link two clusters. To support this operation clustering terminates cluster head nodes broadcast link state message containing the identifier of their next hop cluster heads as well as gateway node to reach the advertised cluster heads. Link state messages are flooded on the network and stored by each node in a local link state database using this database each node is able to maintain information about the topology of the overlay defined by the cluster heads. Node can always find the available low coupling routes between itself and given target cluster ID all paths that do not share cluster heads other than the destination cluster head of the source node.

IV. CLUSTERING

Clustering grouping similar items in one cluster and dissimilar objects in other cluster to achieve efficient multipath routing. Identify unique ID and knows the ID of its neighbors, once the message sent by a node is received correctly within a finite time by all its neighbors, topology of the network does not change during the algorithm execution. Cluster consist of two ways one controls how cluster are formed and second controls how nodes dynamically migrate to reduce cluster overlap. This clustering does not require synchronization therefore nodes can start the protocol in different directions during the protocol nodes respond immediately to message from other nodes but will only select at random intervals to avoid collisions. Cluster heads are cluster leaders and when a node associates with a cluster head it becomes clustered.

Protocols provides the large amount of overhead to achieve clustering we reduce the minimizing flooding minimizing the length of data messages minimizing the processing effort needed to find the maximum number of non-interfering paths.

If the packet arrives at a cluster head it will save the information contained in the message and then broadcasts the packet including the address of the gateways it reach other clusters that are reached through that gateways.

If a cluster node receives a topology message it saves the information it advertises and then discards the message immediately.

A node receives a broadcast packet and its address is included in the gateway list it retrieves the next cluster from the message and searches for its cluster head or the next gateway to reach the cluster.

If the packet arrives at a cluster head node and it already received the packet it is dropped.

NP hard Problem: NP hard is non deterministic polynomial time in computational complexity theory is a class of problems that are informly at least as hard as the hardest problems in NP. Problem H is NP hard if and only if there is an NP complete problem L that is polynomial time turing reducible to H.

Problem H is at least as hard as L because H can be used to solve L.
L is NP complete and hence the hardest in class NP also problem H is at least as hard as NP but H does not have to be in NP and hence does not have to be a decision problem.

NP complete problem transform to each other by polynomial time many one reduction all NP complete problems can be solved in polynomial time by a reduction to H thus all problems in
NP reduce to H however this involves combining two different transformation from NP complete decision problems to NP complete problem L by transformation and from L to H by polynomial turing reduction.

If there is a polynomial algorithm for any NP hard problem then there are polynomial algorithms for all problems in NP and hence P = NP.

If P not equal to NP then NP hard problem have no solutions in polynomial time while P = NP does not resolve whether the NP hard problems can be solved in polynomial time.

If an optimization problem H has an NP complete decision version L then H is NP hard.
Network connections between any two groups of system fail simultaneously systems on both sides of the partition can restart applications from the other side resulting in duplicate services or spilt brain occurs when two independent systems configured in a cluster assume they have exclusive access to a given resource.

V. PROBLEM DEFINITION

Establishment of provable multi path wireless routing protocols, conversion on different activities such as business education entertainment attractive. Transferring thedata by routing protocols associated with multipath to provide the confidential security from attack unauthorized users, to capture a subset of nodes such that no more than certain amount of traffic from source nodes reaches the gateway. Protect from attack will install software tools the system became more complex to avoid all these issues we analyzed blocking protocol algorithm NP hard problem is exponentially hard for the adversary to optimally secure in attacks such as node isolation, network partitioning.

Comparative Study

Multipath traffic routing protocols in wired networks are deemed superior over conventional single path protocols in terms of both enhanced throughput and robustness. Wireless networks though the dynamic nature

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 11, May 2014

of networks and resource constraints entail additional overhead in maintaining and reconfiguring multiple routes which could offset the advantage in wired networks blocking node isolation and network partitioning type of attack are easy to launch are effective in the wireless network domain due to channel constraints and dynamic network topologies. Comparing the existing system we identify the minimum cost blocking problem consider minimum cost blocking in wireless setting problem is applicable to other wireless or wired network. Test results the hardness of problem minimum cost blocking is NP hard for the low no node mobility scenario and P-hard for networks with patterned node mobility. Approximation algorithm for the best case scenario and the performance testing is different settings through random graphs based experiments. Our work analyzes the superiority of multipath protocols over traditional single path protocols in terms of resiliency against blocking and node isolation type attacks especially in the wireless networks domain.

VI. CONCLUSION

Our paper presents blocking of attacks in wireless network in secure manner which evaluate the normal or abnormal activities and also the comparison of proposed solution. Cryptography only protect the message in the packet our analysis NP hard problem is routing protocol that blocks the abnormal activities such as Network partitioning Node isolation in routing discovery which compromise the system from critical condition. Our future work extends more on implementation of secure computing.

REFERENCES

[1] W.Dai,Crypto++Benchmarks.[Online].Available:http://www.cryptopp.com/benchmarks.

[2] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wirelessnetworks," in Mobile Computing, vol. 353. Norwell, MA: Kluwer, 1996, pp. 153–181.

[3] J. Kong and X. Hong, "ANODR: Anonymous on demand routing withuntraceable routes for mobile ad-hoc networks," in Proc. 4th ACM Int.Symp. Mobile Ad Hoc Netw. Comput. 2003, pp. 291–302.

[4] S. Li and A. Ephremides, "Anonymous routing: A cross-layer couplingbetween application and network layer," in Proc. CISS, Mar. 2006, pp. 22–24.

[5] W. Lou and K. Ren, "Security, privacy, and accountability in wirelessaccess networks," IEEE Wireless Commun. Mag., vol. 16, no. 4, Aug. 2009.

[6] Microsoft, Self-Organizing Neighborhood Wireless Mesh Networks.[Online]. Available: http://www.research.microsoft.com/mesh/.

AUTHOR BIOGRAPHY

Arvind Tudigani M.Tech (IT) from AAIDU, Allahabad, B. Tech (IT), JNTU, and Hyderabad He is having 8+ years of experience in teaching currently working as Asst Prof for Osmania University Hyderabad has guided many UG & PG students. His research areas include Distributed Systems, Network Security, and Design Patterns.

Ch. Raju M.Tech Computer Science and Engineering fromJNTUH MS.Is from Osmania University BCA from Osmania University. He is having 8+ years of experience in teaching currently working as Asst Prof for Osmania University Hyderabad has guided many UG & PG students. His research areas include Distributed Systems, Network Security, and Design Patterns.

Thirupathi Marupaka pursuing M.Tech Computer Science Engineering from IETEB.E from Osmania University He is having 5 years of experience in teaching currently working as Asst Prof for Osmania University Hyderabad has guided many UG & PG students. His research areas include Distributed Systems, Network Security, and Design Patterns.