ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 7, July 2013

Literature Survey on latest research issues in MANET

Mrs.Padma .P
Rangareddy, Hyderabad,India

Mr.R.Suresh
Rangareddy, Hyderabad, India

Mobile Ad-hoc Networks (MANET) is an emerging area of research. Most current work is centered with different issues. This paper discusses the issues associated with data communication with MANET, Security in MANET, Intrusion detection. A mobile adhoc network consists of mobile nodes that can move freely in an open environment. Communicating nodes in a Mobile Adhoc Network usually seek the help of other intermediate nodes to establish communication channels. A number of challenges like open peer-to-peer network architecture, stringent resource constraints, shared wireless medium, dynamic network topology etc. are posed in MANET. As MANET is quickly spreading for the property of its capability in forming temporary network without the aid of any established infrastructure or centralized administration, security challenges has become a primary concern to provide secure communication. In this paper we also focus on Intrusion detection system(IDS) and also tried to elaborate on security attacks, IDS architectures, and different intrusion detection mechanisms.

Key Words and Phrases: Web personalization, Web usage mining, user profiling, WWW

1. INTRODUCTION

A traditional mobile network consists of a fixed network of servers and clients, with a collection of mobile clients that move throughout the geographic area of the network. Within the mobile network, servers have unlimited power and communicate with mobile hosts over a wireless connection. Mobile clients may only communicate among themselves through a server. Among the issues in this type of network are client power consumption, connectivity of the network, and reachability of mobile clients from a server. In contrast, a MANET is a collection of mobile servers and clients. All nodes are wireless, mobile and battery powered [1]. The topology can change frequently. The nodes organize themselves automatically, and can be a standalone network or attached to a larger network, including the Internet [2]. All nodes can freely communicate with everyother node. In addition to the issues associated with a mobile network, the power consumption and mobility of the server(s) must also be considered in a MANET. Originally called Mobile Packet Radio, Mobile Ad-hoc Network (MANET) technology has been an important military research area [4]. This technology has practical use whenever a temporary network with no fixed infrastructure is needed. Other uses include rescue operations and sensor networks [3]. The support of these military and civilian uses often requires the presence of a database to store and transmit critical mission information such as inventories and tactical information. There is one other crucial characteristic of a MANET. Traditional mobile networks involve the server in all data communication. MANET includes the traditional database capabilities of data push and data pull, but it also allows the clients to communicate directly with each other without the involvement of the server, unless necessary for routing [3].

MANETS are more vulnerable to attacks than wired networks due to open medium, dynamically changing network topology, cooperative algorithms, lack of centralized monitoring and lack of clear line of defense. Security is a process that is as secure as its weakest link. So, in order to make MANETs secure, all its weak points are to be identified and solutions to make all those weak points safe, are to be considered. Some of the weak points and solutions to strengthen them are considered in this article. However the list is possibly incomplete, and some more weak points of MANETs are likely to be discovered in near future. So Security issues in MANETs will remain a potential research area in near future.

Node mobility on MANET cannot be restricted. As results, many IDS solutions have been proposed for wired network, which they are defined on strategic points such as switches, gateways, and routers, can not be implemented on the MANET. Thus, the wired network IDS characteristics must be modified prior to be implemented in the MANET.

2. MANET ARCHITECTURE

The nodes in a MANET can be classified by their capabilities. A Client or *Small Mobile Host (SMH)* is a node with reduced processing, storage, communication, and power resources. A Server or *Large Mobile Host (LMH)* is a node having a larger share of resources [1]. Servers, due to their larger capacity contain the complete DBMS and bear primary responsibility for data broadcast and satisfying client queries. Clients typically have sufficient resources to cache portions of the database as well as storing some DBMS query and processing modules [1]. As both clients and servers are mobile, the speed

at which the network topology changes can be rapid. A variety of techniques have been proposed to assist in the routing tasks of MANET. New protocols were necessary as the protocols for fixed infrastructures and static networks do not perform well when node mobility is included [8]. A global routing structure is also not useful in MANET due to its dynamic topology and need for distributed control [8]. Work on routing is ongoing and is coordinated through the Internet Engineering Task Force (IETF).

MANET characteristics include a preference for reactive (on-demand) routing, unpredictable and frequent topology changes and distributed control [7]. The primary MANET limitations remain limited bandwidth and battery power [7].

Nodes may not remain connected to the network throughout their life. To be connected to the network, a node must be within the area of influence of at least one other node on the network and have sufficient power to function.

In Figure 1, a few nodes of a MANET are shown graphically. It is important to note that each node has an area of influence. This is the area over which its transmissions can be heard. A LMH will initially have a larger area of influence as it generally has a more powerful battery. As the power level decreases, the area of influence of any node will shrink. This is due to the fact that the power available to broadcast is reduced.

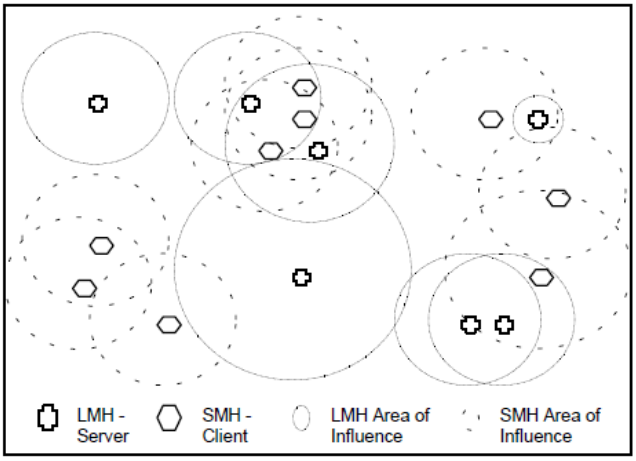

Figure 1: Nodes of a MANET.

Network nodes may operate in any of three modes that are designed to facilitate the reduction in power used [9]:

∗ Transmit Mode: this is the mode using the most power. It allows both the transmission and reception of messages and consumes 3000 to 3400 mW [9].

∗ Receive Mode: the CPU is capable of processing information and is also capable of receiving notification of messages from other nodes and listening to broadcasts. 1500 to 1700 mW are consumed in this mode [9].

∗ Standby Mode: the CPU does no processing and the node has no ability to send/receive messages. The node is inactive and consumes only 150 to 170 mW [9]. This mode allows a node to turn itself off for short periods of time without requiring power-up or re initialization. A node with no remaining power, or one that is off, is not currently a part of the network.

It is clear from the description and Figure 1 that a node may not be reachable by another node (LMH or SMH). In other words, nodes may become disconnected from the entire network. When moving back in range of other nodes, they will become reconnected. Conversely, a node may be reachable by several LMHs or SMHs. The potentially rapid and regular reconfiguration of the network topology is routine with the MANET.

Mobile Ad-Hoc Databases

A MANET may include data pull, data push and peer-to-peer communication. No research has been done which includes all three forms of communication. However, data push and data pull have been addressed to varying degrees. Below the recent work in Mobile Ad-Hoc data communication is addressed.

Wieselthier, et. al. have been working together on MANET broadcast issues. Their approach is the construction of a minimum-energy tree rooted at the broadcast source [6]. Two algorithms called Broadcast Incremental Power (BIP) and Multicast Incremental Power (MIP) have been advanced for building these trees. The BIP builds the minimum energy tree for a broadcast, while the MIP uses the BIP algorithm, but only includes those branches necessary to reach the clients needing to receive a specific broadcast [6].

The algorithms were tested and showed that by utilizing broadcast in a mobile environment, energy savings can be achieved. Further studies with larger networks were recommended [6]. However, node mobility was not addressed. The cost of building the tree is considered negligible by the authors as the use of the tree is long when compared to the building of the tree [6]. This would be the case for stationary nodes. However, stationary nodes would be the exception in MANET. They accommodate “movement” with the observation that increasing transmitter power will allow them to reach nodes in new locations. No potential interference between broadcasts and no need to rebuild the tree once created are considered. The restrictions and assumptions are limiting. In addition, tree-based protocols do poorly with node mobility. The problems of limited bandwidth, the need for tree maintenance, and node mobility remain.

Two algorithms to handle data push and data pull within the MANET were proposed in [1]. The first is the adaptive broadcast scheduling algorithm. Within this algorithm there are two potential ways to construct a broadcast. New items may be either added to the algorithm or may replace less important data items [1].

A global network where all servers in a region know the location and power of all other servers in the region and full replication of the database is assumed. Periodically, each server broadcasts its location and power level. This begins the broadcast cycle [1]. This is a soft real-time system. There are deadlines for data delivery. The deadlines were used to determine which data request to service although no penalty for missing a deadline was mentioned. There is a leader protocol that selects the server in a region with the greatest remaining power. The leader coordinates the broadcast responsibilities of other servers in its area of influence [1]. The lead server determines which portion of a broadcast each

server transmits. The power level of each server drives this broadcast assignment. The server with the least power transmitted the most important data items[9]. No server transmits the entire broadcast unless it is the only server in a region After the conclusion of broadcasting, clients are permitted to query the servers. After the time period for queries, the broadcast cycle repeats [1].
This initial algorithm has a potentially large communication overhead, servers with no clients still broadcast, and less popular items may starve or be broadcast too late [1].
The second algorithm utilizes a popularity factor (PF), as suggested by Datta et. al. [7]. The PF is a measure of the importance of a data item. The PF increases each time a request is made for a data item [1]. The amount of time since the request was made also affects the PF. If it has been too long, the need to broadcast the item may be gone. This factor is called the Resident Latency (RL) and is system and
scenario specific [1]. The PF decreases whenever a request exceeds the RL value [1]. The PF is used to assist in the building of relevant broadcasts and includes RL in order to make allowances for the movement of nodes. When the PF of broadcast items is high, the probability of a broadcast that serves maximum needs increases. If a server has not received any requests for a certain number of broadcasts, it will sleep rather than broadcast to an empty audience [1]. Finally, to localize data delivery, the lead server assigns each server the amount of data to broadcast but not the items to broadcast [9].
To deal with insufficient power levels, the servers rebroadcast the previous index and broadcast if they have insufficient power to build a new broadcast [1]. It is not clear why broadcasting old information is preferable to no broadcast at all.
This approach is still not sufficient as servers can be assigned a broadcast larger than their power levels would permit. Power and bandwidth is also wasted with duplication

4. SECURITY PROBLEMS IN MANETs

MANETs are much more vulnerable to attack than wired network. This is because of the following reasons:
Open Medium - Eavesdropping is more easier than in wired network.
Dynamically Changing Network Topology – Mobile Nodes comes and goes from the network, thereby allowing any malicious node to join the network without being detected.
Cooperative Algorithms - The routing algorithm of MANETs requires mutual trust between nodes which violates the principles of Network Security.
Lack of Centralized Monitoring - Absence of any centralized infrastructure prohibits any monitoring agent in the system.
Lack of Clear Line of Defense - The only use of I line of defense - attack prevention may not suffice. Experience of security research in wired world has taught us that we need to deploy layered security mechanisms because security is a process that is as secure as its weakest link. In addition to prevention, we need II line of defense - detection and response.
The possible security attacks in MANETs can be divided into two categories:
Route Logic Compromise: Incorrect routing control messages are injected into the network to damage routing logic.
Traffic Distortion Attack: All attacks that prohibits data packets to transfer from the source to the destination, either selectively or collectively comes under the category of Traffic Distortion Attack.
This type of attack can snoop network traffic, manipulate or corrupt packet header or contents, block or reply transmissions for some malicious purposes.

Security Analysis
Passive attack: Malicious nodes cannot find the sender, receiver and other intermediate node just by eavesdropping on path discovery messages.
Active attack: Any modi_cation of the path discovery messages will be detected by receiver because of signatures appended, which preserves integrity of message.
Denial of Service Attack: The protocol is incapable of resisting DOS attack involing flooding the network with meaningless path discovery messages.
It is because verification of these messages involves complex computations which is resource consuming. Also it consumes network bandwidth. In fact DOS attack is very difficult to resist in any protocol.

5. INTRUSION DETECTION IN MANETs

Intrusion Detection systems (IDS) serves as second line of defense, after first line of defense by prevention techniques. The two major analytical techniques in intrusion detection are
Misuse detection: It uses signature of known attacks, to identify those attacks
Anomaly detection: It uses established normal profiles only to identify any unreasonable deviation from them.
Architecture of an IDS agent
Figure 2 shows the architecture of an IDS agent that can be deployed on each mobile node. The various components are:
Data Collection Module : It collects various security related data from various audit data sources and preprocess them to the input format of detection engines.
Detection Engine: It determines whether a particular state of system is anomalous, based on predetermined normal profile of network created during training process.
Local Aggregation and Correlation Engine (LACE): It aggregates and correlates various detection results and transfer them to GACE.
Global Aggregation and Correlation Engine(GACE): Its function to aggregate detection results from a number of nodes and globally make decision about any malicious event.

Routing anomalies in MANETs

This subsection will describe how Routing anomalies can be detected in MANETs. One important assumption of intrusion detection is that normal and intrusive behaviors are distinguishable.

The following are the challenges in routing anomaly detection

Due to arbitrary mobility, it is very difficult to establish a mathematical model to characterize routing disruption attack. Difficulty in distinguishing Routing control packets generated by attacker, and that by mobility induced error.

In this sub-section, a Markov Chain Based Anomaly detection scheme is briey described. The following steps are required

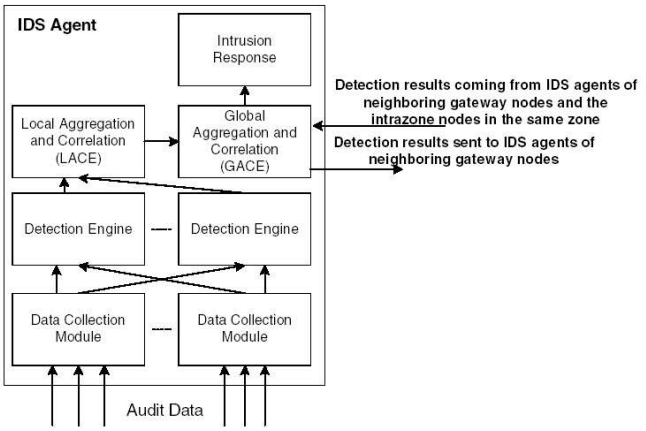

Figure 2: IDS Agent.

Feature Selection

Features are the attributes of data that needs to be considered. Features associated with routing caches of mobile nodes are determined in order to characterize their normal changes. Two main features are used.

PCR: % Change in number of routing entries in certain time periods.

PCH: % Changes in sum of hops of all routing entries in a certain time periods

Markov Chain Based Intrusion Detection

The idea of using this model is that the routing changes in mobile nodes can be considered as random process with stationary transition probabilities of Markov Chain. This statement is valid for a particular class of network, whose normal traffic follows a regular pattern.

Two step process of Intrusion Detection are following:

1. Markov Chain Model Construction

The Markov Chain Model Construction requires some amount of training data representing normal traffic pattern of the network. During construction process, the training data is preprocessed for discretization, and divided into set of traces. Each trace has a continuous values of statistical feature that we want to consider. A virtual window of size W slides through this trace. At each position of window the transition of W ordered states (feature values) within the window to new state, which is the feature value just on the right of window, is recorded. This process, if repeated for large number of traces. This will build a comprehensive probability model for a particular network traffic. This model can be used to calculate the probability of a given W + 1 number of ordered feature values.

2. Classifier Construction

The Classifier of Markov Chain Model is constructed after training the model. The classifier determines how anomalous is a given trace of statistical feature values. Under operational condition, the traces from the routing caches are recorded and fed to the detection engine.

The detection engine runs the classifier over this trace. It involves sliding a virtual window of length W, and find out the probabilities of every continuous W + 1 feature value of the trace. We get a set of probabilities as (P_0; P_1; P_2; :::; P_k). The lesser is the value of these probabilities, the more anomalous are the events that these probabilities are representing. Now, either we can calculate the average probability and compare it with some threshold or we can analyze individual probabilities. The later approach of analyzing individual probabilities is better because calculating average probability can suppress some of the few exceptionally low probabilities.

Some of the approach to analyze these probabilities is:

A common approach is to individually compare the probabilities with some threshold value. If some probability is less than a particular threshold, then raise an alert. The ratio of cumulative sum of probability with number of probabilities that are summed is compared with some threshold at each iteration of summation. Again if the ratio becomes less than some threshold at any stage, an alert is generated. Selecting the threshold T determines a tradeoff. Higher value of T will increase the anomalous detection ratio, but may also increase the false alarm ratio. Lower value of T will decrease the false alarm ratio but it will also decrease detection ratio. A proper value of T can be determined empirically, with desired level of trade-off.

There are some limitations of this model:

- Unexpected changes in statistical features are undesirable, as they introduce noise in the probability model.
- Overhead of training data is significant.

6. MISBEHAVIOUR DETECTION THROUGH CROSS-LAYER ANALYSIS

Some *smart* attackers may simultaneously exploit several vulnerabilities at multiple layers but keep the attack to each of the vulnerabilities stay below the detection threshold so as to escape from capture by the single-layer misbehavior detector. This type of cross-layer attack will be far more threatening than the single-layer attack in that it can be easily skipped by the single-layer misbehavior detector. Nevertheless, this attack scenario can be detected by a cross layer misbehavior detector, in which the inputs from all layers of the network stack are combined and analyzed by the cross-layer detector in a comprehensive way. First of all it will be an important problem that how to make the cross-layer detection more efficient, or in other words, how to cooperate between single-layer detectors to make them work well. Because different single-layer detectors deal with different types of attacks,

there can be some different viewpoints to the same attack scenario when it is observed in different layers.
Therefore it is necessary to figure out the possible solution if there are different detection results generated by different layers. Second, we need to find out how much the system resource and network overhead will be increased due to the use of cross-layer detector compared with the original single layer detector. Due to the limited battery power of the nodes in the ad hoc networks, the system and network overhead brought by the cross-layer detection should be taken into account and compared with the performance gain caused by the use of cross-layer detection method.

7. CONCLUSION AND FUTURE SCOPE OF RESEARCH.

The following conclusions are made based on the study communication and security and Intrusion detection in MANET's.
The data communication research issues in MANET databases center around two areas. The first area concerns the limitations of the environment (wireless, limited bandwidth, battery powered). The second area concerns the many ways in which data communication may take place. Data communication is an important topic that needs to be addressed when designing database systems in MANET environments. This topic involves far more than network routing. In addition, existing mobile protocols are insufficient. They are not geared towards the specialized needs of a MANET. The areas of concern within MANET data communication are raised. Future research will need to begin to address these issues. Due to the mobility and open media nature, the mobile ad hoc networks are much more prone to all kind of security risks, such as information disclosure, intrusion, or even denial of service. As a result, the security needs in the mobile ad hoc networks are much higher than those in the traditional wired networks. Because of the emergence of the concept pervasive computing, there is an increasing need for the network users to get connection with the world anytime at anywhere, which inspires the emergence of the mobile ad hoc network. However, with the convenience that the mobile ad hoc networks have brought to us, there are also increasing security threats for the mobile ad hoc network, which need to gain enough attention

REFERENCES

[1] Gruenwald, L., Javed, M., and Gu, M. Energy- Efficient Data Broadcasting in Mobile Ad-Hoc Networks. In *Proc. International Database Engineering and Applications Symposium (IDEAS '02)*, July, 2002.
[2] Section 2.5.3. In *Proc. 54th Internet Engineering Task Force* July, 2002.
[3] Kahn, J., Katz, R., and Pister, K. Next Century Challenges: Mobile Networking for "Smart Dust". In *Proc. 5th International Conf. on Mobile Computing and Networking (MOBICOM '99)*, pp. 271-276, August, 1999.
[4] Corson, M., Freebergyser, J., and Sastry, A., "Mobile Ad Hoc Networking: Editorial," *Mobile Networks and Applications*, 4(3): pp. 137-138, 1999.
[5] Aksoy, D. and Franklin, M. Scheduling for Large- Scale On-Demand Data Broadcasting. In *Proc. 12th International Conf. on Information Networking* pp. 651-659, January, 1998.
[6] Wieselthier, J., Nguyen, G., and Ephremides, A., "Algorithms for Energy-Efficient Multicasting in Static Ad Hoc Wireless Networks," *Mobile Networks and Applications*, 6(4): pp. 251-263, 2001.
[7] Liu, J., Zhang, Q., Li, B., Zhu, W., and Zhang, J., "A Unified Framework for Resource Discovery and QoS-Aware Provider Selection in Ad Hoc Networks," *ACM Mobile Computing and Communications Review*, 6(1): pp. 13-21, 2002.
[8] Lee, S., Su, W., and Gerla, M., "Wireless Ad Hoc Multicast Routing with Mobility Prediction," *Mobile Networks and Applications*, 6(4): pp. 351-360, 2001
[9] Singh, S., Woo, M., and Raghavendra, C. Power Aware Routing in Mobile Ad Hoc Networks. In *Proc. 4th International Conf. on Mobile Computing and Networking (MOBICOM '98)*, pp. 181-190, October, 1998.
[10] Satria Mandala, Md. Asri Ngadi, A.Hanan AbdullahA Survey on MANET Intrusion Detection., International Journal of Computer Science and Security, Volume (2) : Issue (1)-2005.
[11] J. Parker, A. Patwardhan and A. Joshi, "Cross-layer Analysis for Detecting Wireless Misbehavior", in *Proceedings of the IEEE Consumer ommunications and NetworkingConference*(*CCNC 2006*), Las Vegas, Nevada, USA, Jan. 2006.