Roaming Honeypots along with IDS in Mobile Ad-Hoc Networks

Sabah Shamsh
Department of Computer Science,
Amity University
Lucknow, India

Vandana Dubey
Lecturer, Dept. of Computer Science,
Amity University
Lucknow, India

ABSTRACT

At the present time, Mobile Ad-Hoc Networks are being used in wide variety of applications, such as, mobile commerce, transportation, sensor networks etc. Hence, secure deployment of MANETs is a necessary condition because MANETs are most vulnerable to attacks. Lots of research has been performed on deployment of IDS in MANETs, but, using honeypots in MANETs is a new concept. Honeypots are used to uncover the motive of attacks on any network. Only one model for using honeypots in MANETs has been proposed by Ali Mirzaei *et al* in Nov, 2012, ISSN 2301-2005. This research mainly focuses on taking the work further by using roaming honeypot technique in MANETs.

General Terms

Security, Mobile Ad-Hoc Networks, Honeypots, IDS

Keywords

MANETs, Roaming Honeypots, Zone-Based MANETs

1. INTRODUCTION

Mobile Ad-hoc Networking is being used in wide variety of applications nowadays. But this mobile technique is still under development and is facing a lot of challenges in developing secure routing protocols as well as maintaining security for communication. Secure communication in MANETs mainly requires trust in the nodes which are participating in maintaining the whole mobile ad-hoc network. This is a very serious issue because the topology of MANET is dynamic i.e., continuously changing and any node can become a part of the network if it is in radio range of any existing node in MANETs [1]. Hence, trusting the new nodes as well as the existing nodes is very difficult because the attacker can launch an attack through a new node or can even compromise the already existing nodes of MANET [1].

A lot of research has already been done to implement Intrusion Detection Systems in MANETs to detect and mitigate attacks, but they do not uncover the motive behind the attack. Discovering and understanding the motive of attack by the attacker can be very beneficial for future studies in MANETs, as well as having the evidence against the attackers for legal benefits. Real-time forensic honeypots have been used for this purpose in wired and wireless networks for a very long time and the concept of deploying them in MANETs have started recently. Lance Spitzner, 2003, defines honeypots as an information system whose value lies in unauthorized and illicit use of that resource [15]. Main purpose of using honeypots is to lure the attacker to interact with it. Honeypot is constructed in a way to be vulnerable to the attacks by luring the attackers with system and application vulnerabilities and false information.

Concept of roaming honeypots is not new for wired networks. It renders the location of honeypots to be hidden to the attacker. The case where the location and presence of honeypots in MANETs becomes known to the attacker is of great disadvantage towards using honeypots because sophisticated attacks are capable of recognizing a honeypot. Hence, using roaming honeypots can be of great advantage to keep the MANETs secure.

This research uses an election mechanism on the basis of which, the group of honeypots can decide whether to act as a normal node to stay disguised or act as a honeypot. The Mobile Ad-hoc network is divided in zones. The election is performed on the basis of density of the nodes in a particular zone of the network because the zone where the network becomes dense has a high probability of attacks. The honeypots with minimum number of nodes surrounding them will act as normal nodes.

The rest of the paper is divided into the following sections: Section 2 gives brief introduction about MANETs, section 3 gives brief introduction of honeypots, honeytokens and roaming honeypots, section 4 gives brief introduction about intrusion detection system, section 5 states the proposed work, section 6 states an architecture proposed for honeypots in MANETs, section 7 states related work, the paper has been concluded in section 8. At the end future scope, acknowledgement and references are stated.

2. MOBILE AD-HOC NETWORKS

Ali Mirzaei studied MANETs and bought the challenges being faced in MANETs in light very well [1]. Mobile Ad-hoc Network or MANET is a self configuring network with no infrastructure which uses wireless communication. This network makes wireless devices such as cell phones, laptops and PDAs capable of forming an Ad-Hoc network among them for wireless communication. These devices are referred to as nodes in the rest of the paper. Each node in MANET is free to move independently in any direction. Hence, the topology of MANETs is dynamic in nature. A node can join or leave the network anytime. Each node acts like a router in MANETs. The scale of MANET network can be large or small i.e., dynamic because any node which is in radio range of any existing node in MANET network can become a part of the network.

MANETs have been applied in many areas where no functional infrastructure is available such as military use and rescue operations. It is also being used in Intelligent Transport System and Vehicular Ad-Hoc networks (VANETs).

Because of self configuring wireless network with no infrastructure available, MANETs pose a potential security threat. There is no centralized management system in MANET; hence, it becomes very hard to monitor the traffic flow. An attacker can join the network freely and can communicate with the other nodes of MANET. Other nodes

can also be compromised by the attacker. An adversary can participate in decision making and can disorder group tasks [1].

Making service available to all nodes in a reliable and secure manner is a major challenge for MANETs. The scale of the network can vary; hence, security mechanism should be able to handle a large network as well as small ones. Topology is changing dynamically, so keeping track of trust relationship poses a great challenge. Limited power supply is also an issue in MANETs [1].

3. HONEYPOTS

"Honeypot are used to monitor the attacker's behavior. It is an information system that lures the bad guys to interact with it. The value of honeypot lies in unauthorized use of that resource [15]." Honeypot lures attackers by giving them false or fake information which appears to be of some use to the attacker. Honeytokens are simplified form of honeypots [1] [14]. They are the resources that can be modified in such a way that if an attacker interacts with them, he is directed to a honeypot. The examples of honeytokens are credit card numbers, excel spreadsheet, a false login etc.

Honeypots require very less resources to run them, so they are easy to use. Through honeypots, events and activities of the attacker on the honeypot are captured, so encryption being used by the attacker will not matter, because there is no need to capture the data being robbed (as it is fake), the only need is to know the resources on the honeypot that the attacker interacted with. The motive of using honeypots is to understand the goal of the attacker. This will be helpful in learning new malicious activities, methods and evidence can be collected against an attack for legal use and network forensics.

3.1 Roaming Honeypots

It is a mechanism that allows the location of honeypots to be unpredictable to the attacker, continuously changing and disguised [2]. The case where location and presence of honeypot becomes known to the attacker is of great disadvantage in using honeypots in MANETs. Using the deception technique of roaming honeypots in mobile ad-hoc networks will render the location of honeypots to be unknown to the attacker. The attacker won't be able to locate a honeypot because the location of honeypot will be random for the attacker. Moreover, a larger part of mobile ad-hoc network can be tracked and monitored using the roaming honeypots scheme.

4. USE OF INTRUSION DETECTION SYSTEM IN MANETS

Intrusion Detection is a security scheme to detect unauthorized use of a resource and take required actions against the suspicious activities to mitigate them. They are being used in MANETs for protecting the network from threats and providing a secure communication in MANETs. Basically, IDS are of two types: misuse-based detection system and anomaly-based detection system [5]. Misuse-based detection technique tries to match the ongoing activity against the known attack signatures while anomaly-based technique searches for a deviation from normal pattern of traffic flow for an attack. An improved technique known as specification based detection technique combines the qualities of misuse-based detection and anomaly-based detection [5].

IDS have been deployed in MANETs for a secure communication [4] [5] [10] [17]. Combining them with honeypots will help to update the database of IDS with new attack patterns and will help in building a more secure and reliable communication in MANETs.

5. PROPOSED WORK

For optimal use of honeypots in MANETs, the roaming technique being used in honeypots can be of great use. It will render the location of honeypot to be unknown to the attacker in MANETs. Here, a scheme has been proposed to apply roaming technique in honeypots to be used in MANETs.

5.1 Division of Network

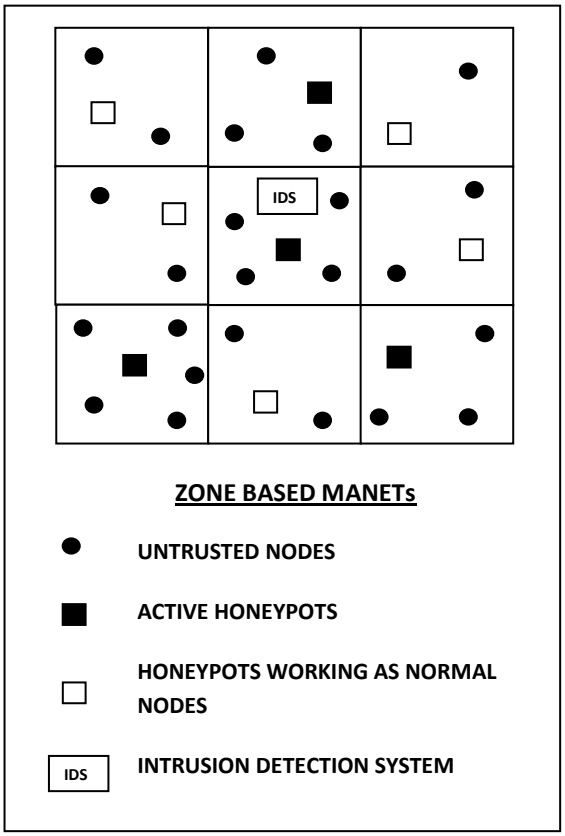

Figure 1: Architecture of Zone-Based MANETs and Honeypots in each zone

The whole network is virtually divided in smaller grid like zones for convenience and one honeypot is deployed in each zone (See Figure 1). The mobile honeypots should be aware of their own positions through a positioning system, for example: GPS. A honeypot can obtain the position of other nodes present in the same zone through location services, some services have been described by J. Li et al in "A scalable location service for geographic ad-hoc routing", *ACM/IEEE Int'l. Conf. Mobile Comp. Net. (MOBICOM)* and by S. Giordano and M. Hamdi in "Mobility management: The virtual home region" *Tech. report*, October 1999 [11][12]. Yu-Chee Tseng *et al* described location awareness in Ad-hoc Wireless Mobile Networks [13].

In Zone-Based approach, the geographical area covered by MANETs is divided into several grids called zones. The two-level zone-based peer-to-peer protocol divides the MANET's

geographic area into zones [13]. Through a GPS receiver, each mobile host knows its current position and thus it's Zone-ID. Through this approach, the MANET's area is divided geographically and honeypot is deployed in each zone. The proposed work is to activate the honeypots of those zones where the network becomes dense.

5.2 Selection of Honeypots and Nodes through Election

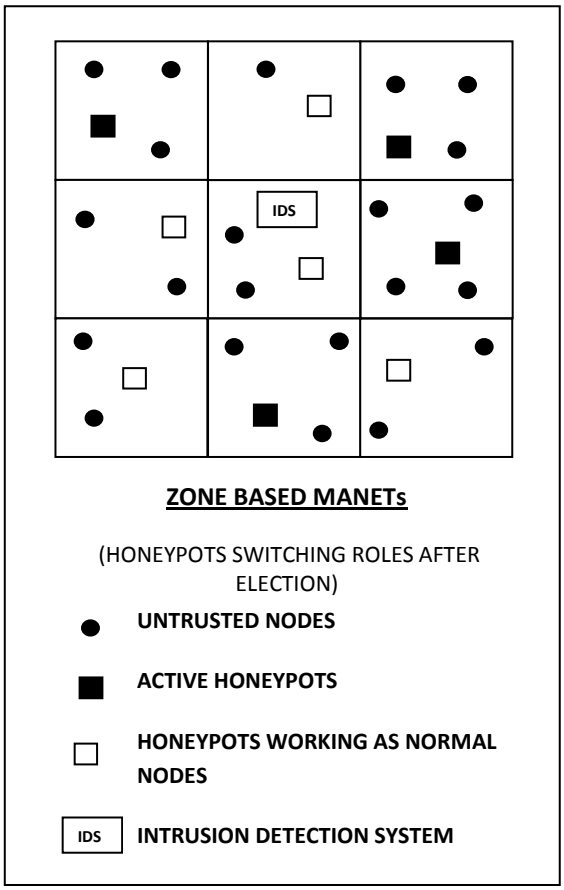

Figure 2: Honeypots switching roles after election

Each honeypot counts the number of nodes in its zone. Based on the total number of nodes surrounding each honeypot, an election is held among the honeypots in a secure manner using encrypted communication described further (See subsection 5.5). The honeypots with minimum number of nodes surrounding them will act as normal nodes and the rest of the honeypots will be active (See Figure 1. and 2.). The decision for a honeypot to act as a honeypot or as a normal node will be on the basis of the average of least dense zone and most dense zone. If the zone density of a zone is more than the average value, the honeypot of that zone will be active and if the zone density of a zone is less than the average value, the honeypot of that zone will act as a normal node. Before a honeypot changes its status from acting as a honeypot to being a normal node, it will drop all its current requests that it is serving to the malicious nodes.

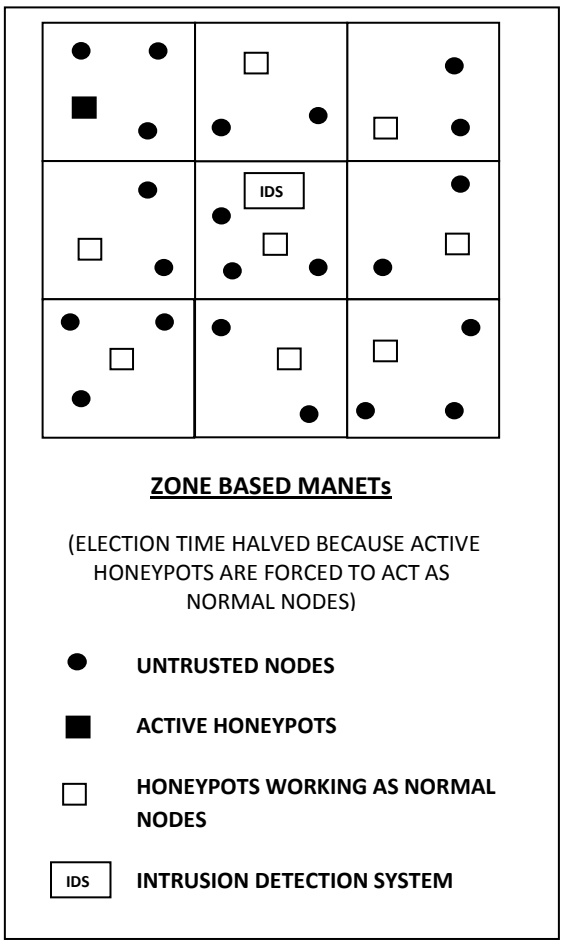

Figure 3: Honeypots forced to act as normal node

5.3 Election after specified duration

As the topology of Mobile Ad-hoc Networks is dynamic in nature, i.e. a node can enter or leave the network anytime, the density of the network might change after sometime. So, the election will be held after a predefined duration of time to choose the two sets: the set of honeypots and the set of honeypots which will now be working as normal nodes participating in MANET network. This time duration is the service duration for the active honeypots. Honeypots which have already been chosen once to act as honeypots for one service duration should not be chosen in the next set. A problem arises at this step, it is possible that the density of a zone may be not change after specific service duration and the honeypot of that zone may be forced to act as a normal node due to the next election when the service duration expires (See Figure 1 & Figure 3.). To mitigate this problem, the service duration time for next service of honeypots should be lessened to half of the actual service duration, so that the next election can be called soon where the previous honeypots can be active again.

5.4 Mechanism to Monitor the Density of the nodes

After specified amount of time, each honeypot including the ones which are working as normal nodes will monitor the density of the zone to which they belong, which will be needed as the data on the basis of which next election among honeypots will be held. GPS system and location services can

be used to monitor the density of the nodes in each zone from time to time.

5.5 Use of ID-based cryptography for secure communication between honeypots

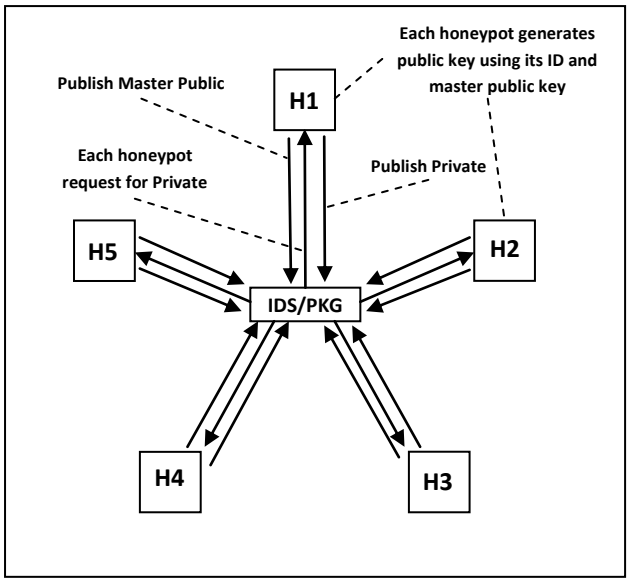

Figure 4: Use of ID-Based Cryptography for Secure Communication

ID based cryptography was first introduced in 1984 by Shamir, A, in "Identity based cryptosystems and signature schemes" [9]. It will be used for secure communication between honeypots in MANETs. Whenever the honeypots would like to communicate among themselves for conduction of election, a secure communication will be needed among them. In ID-based cryptography, a trusted third party which is a Private Key Generator (PKG) generates private keys using asymmetric encryption for a node which wants to communicate [10]. In the process, PKG first generates a master public-private key pair. It publishes the public key called the master public key to the honeypots present in the network and retains the private key called the master private key to itself (See Figure 4.). A honeypot can generate its own public key from its ID using the master public key of PKG. Then the honeypot will contact the PKG to obtain its private key. The private key is generated by PKG using the master private key. The IDS module in the proposed work is used as the private key generator for the honeypots.

The keys generated above are used for authentication of honeypots. Now when a honeypot H1 would like to send a message to honeypot H2, such that only H2 can decrypt the message and make sure that the message was really from H1, H1 will sign the message using its private key and now encrypt the message using the public key of H2. When H2 receives the message, it first decrypts it using the private key and again decrypts it using public key of H1. If the verification succeeds, the honeypot accepts this message as valid. This idea had been taken from the work of F. R. Yu *et al* [10].

5.6 Use of Intrusion Detection System in MANETs

The idea of using honeypots along with Intrusion Detection System in cluster based MANETs was introduced by Ali Mirzaei *et al*, 2012 [1]. In this scheme, the information collected by roaming honeypots is sent to update the database of attacks maintained by IDS. This can be carried out using a secure communication between honeypots and IDS through the same asymmetric encryption technique as discussed earlier. For this, IDS will also generate its own public key using its ID to communicate with the honeypots. PKG module is being added to IDS because each honeypot communicates with it to update the database of known attacks maintained by IDS.

6. MODULES IN ROAMING HONEYPOT

Each honeypot node in this roaming scheme will consist of the following modules used by Ali Mirzaei with some more modules to customize it for roaming [1], because it has all the elements required for a classic deployment of honeypot with little changes to make it suitable for roaming environment.

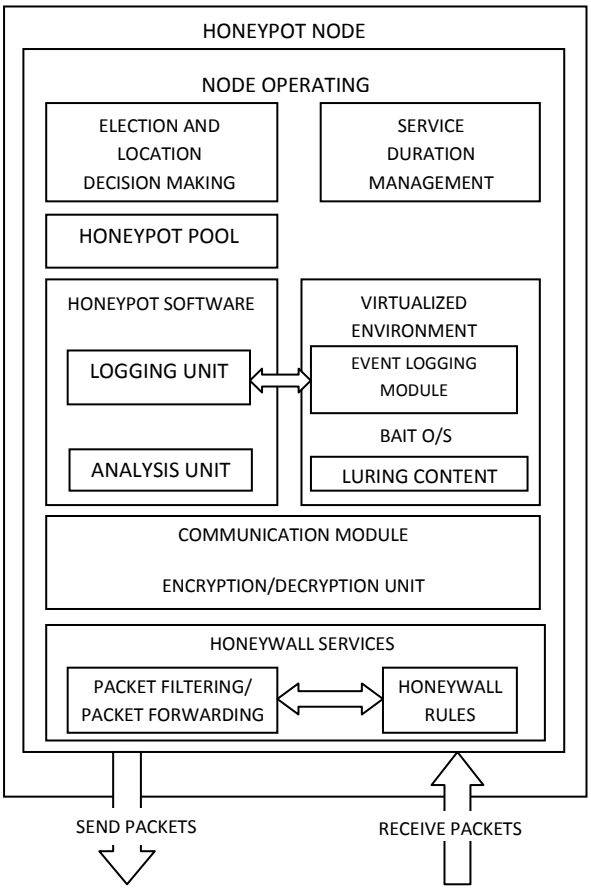

Figure 5: Honeypot Modules

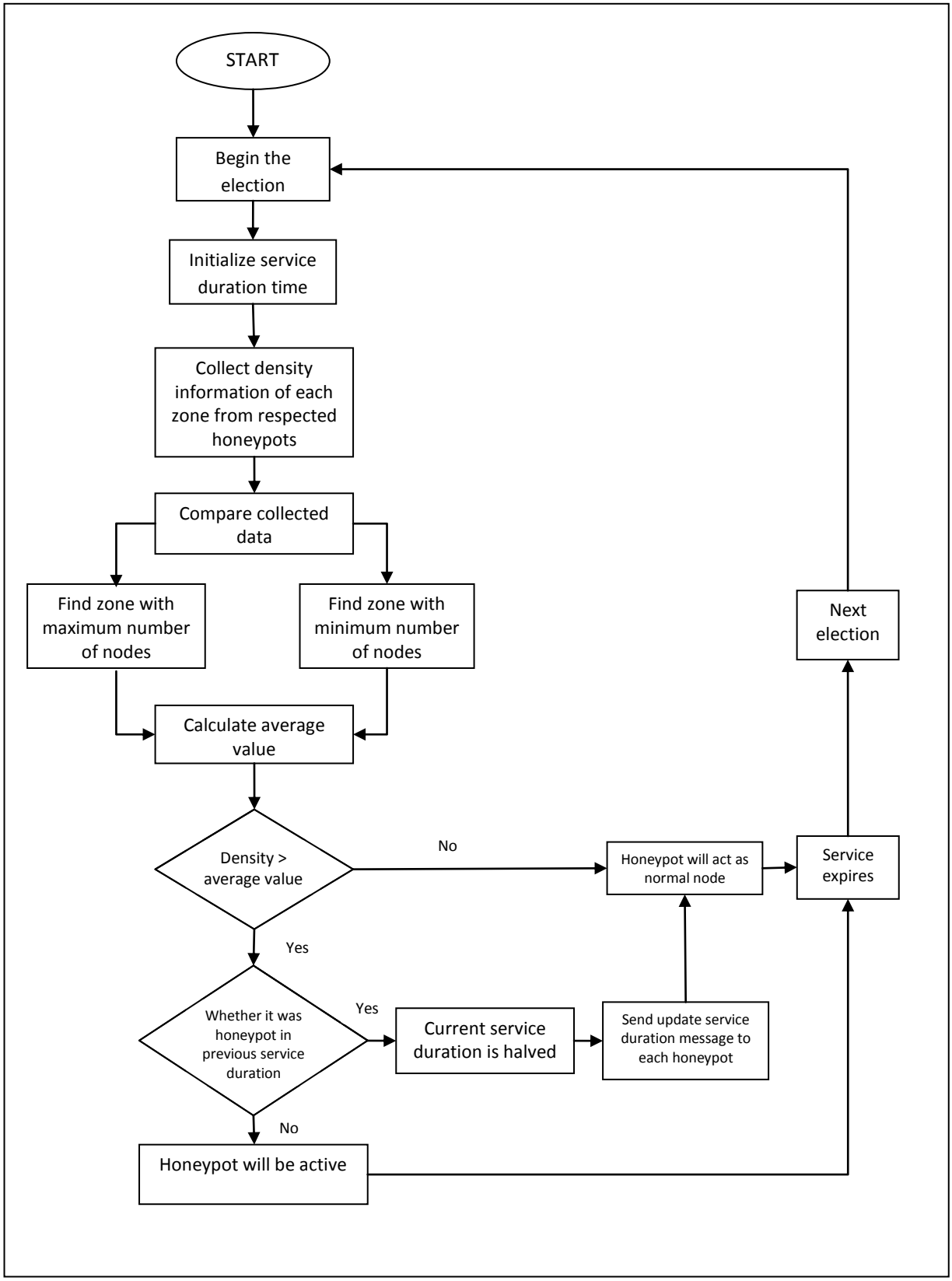

Figure 6: Procedure of Election

6.1 Basic Modules

6.1.1 Node Operating System

It is the host operating system running on honeypot node which supports guest operating system. It also supports module for conduction of election and for deciding the state in which the honeypot should run, i.e., as a honeypot or a normal node. It also manages service duration of the honeypot/normal node. Beside this, it also has a honeypot pool for keeping track of honeypots, honeypot software, communication module for safe interaction and honeywall service [1].

6.1.2 Bait Operating System

It is the guest operating system which the attacker takes for a vulnerable operating system with which he can interact to gain sensitive information which is actually false. It consists of vulnerabilities which renders the honeypot to seem vulnerable for an attack to the attacker. It mainly has an event logging service to log all the activities of the attacker [1].

6.1.3 Luring Content

This is the false content which the attacker is searching for [1].

6.1.4 Honeypot Software

It is the software which logs the activities of the attacker. It analyses the data collected from event logging service [1].

6.1.5 Honeywall Service

This service runs on the host operating system. All the incoming and outgoing traffic of the honeypot node passes through it. Packets passing through the honeywall can be of the following kinds [1]:

6.1.5.1 Another Destination

Packets going to another destination using honeypot as an intermediate node: These packets just need to be forwarded to the next node based on the routing protocol currently in use.

6.1.5.2 Addressed to Honeypot

Packets having the honeypot IP address as destination: These can also be of two types, the source IP address is IDS or the source IP address is some other random node. When the source is IDS, a verification of source is done and confirmed. Then the packet is sent to the honeypot for use. When source is some other random node, then the packet is sent to the bait operating system and the activities are logged.

6.1.6 Event Logging Module

This is basic module of honeypot which records all the activities of the attacker and maintain logs of each activity done by each attacker.

6.2 Modules Required for Election

6.2.1 Service Duration Management Module:

This module decides the time duration allotted to a honeypot after which next election will be done. The service duration time can be chosen on the basis of the environment where the MANET is being deployed. If the environment is very critical, then a small value for service duration can be chosen.

6.2.2 Election and Location Decision Making Module

It decides which honeypot should be active after election based on the density of the network.

The procedure for election has been described in figure 6 (See Figure 6 on previous page.), these are the steps to be followed by each honeypot node to decide whether to act as a honeypot or a normal node:

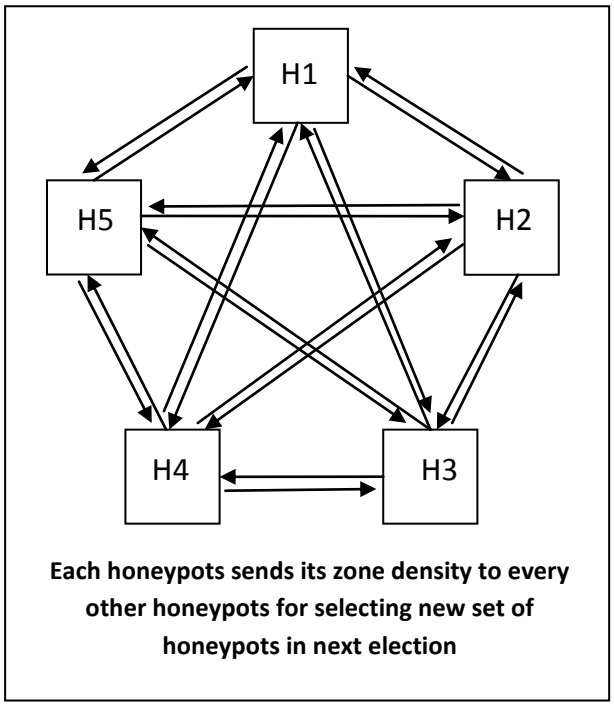

Figure 7: Election between Honeypots

6.3 Module Required for Roaming

6.3.1 Honeypot Pool

It keeps track of all the honeypots in MANETs as well as update location of current honeypots and nodes through update messages and GPS services. These update messages are sent in a secure manner to each honeypot using ID-Based cryptography. It will also contain the IDs of the honeypots in MANETs.

6.3.2 Communication Module

It is responsible to build a secure connection among honeypots to interact with each other and with the Intrusion detection System. This module will use the ID-Based cryptography described above for the secure communication.

7. RELATED WORK

Although much work has been done in implementation of Intrusion Detection System in MANETs but very less work has been done for implementing honeypots in MANETs.

A model for honeypots has been proposed by Ali Mirzaei *et al* in 2012, for their use in Cluster-Based MANETs along with Intrusion Detection System [1]. It consists of node operating system, bait operating system, luring contents, honeypots software and honeywall services.

Intrusion Detection System using Traffic Prediction has been proposed for Wireless Industrial Networks by Min Wei and Keecheon Kim in June, 2012. They proposed a data traffic prediction model based on autoregressive moving average (ARMA) using the time series data. The model can quickly and precisely predict network traffic [4].

Roaming honeypots have been used for mitigating denial-of-service attacks. In denial-of-service attacks an attacker takes service from a victim server at a high rate. The roaming honeypots scheme detects and filters external attacks and also mitigates internal attacks. It does so by dropping all connections when a server switches from honeypot state into server state [2].

Many Intrusion Detection Techniques have been developed for Mobile Ad-Hoc Networks. Intrusion Detection Techniques are generally of two types – misuse detection techniques and anomaly detection techniques. Specification based techniques are an improvement over the above two techniques because it combines the advantages of anomaly detection and misuse detection [5]. Zhang *et al* [6] have proposed Intrusion Detection Techniques for use in Wireless networks to make a large group of anomaly detection models using two classifiers, RIPPER and support vector machine (SVM) Light. Similarly, Huang *et al* [7] introduced a learning based method which uses cross feature analysis to detect and capture correlation patterns. Huang and Lee [8] have proposed a mechanism where one node can collaborate with its neighbors and initiate a detection process over a broad range.

The *Honeypot Project* was founded in the year 1999. Since then, honeypots are being used to monitor the attacker's activities. HoneySpot, a wireless honeypot which was known as T*he Spanish Honeypot Project* was designed for monitoring attacker's activities in wireless networks. The architecture of wireless honeypots worked on 802.11 wireless network standards [3].

In 2006, T*he MAP Project* was introduced. The concept was to – Measure, Analyze and Protect the network and to develop a framework to address attacks on Wi-Fi networks [3].

In 2007, Raytheon sponsored a project on wireless honeypots named - *The Hive*, to analyze wireless threats. The project is used on Linux environment. It provided access point capabilities and network simulation through Honeyd [3].

Suen Yek proposed a method to use deception technique to implement network defense using a wireless honeypot [18]. He utilized deception-in-depth concept to implement integrated wired and wireless honeypots and tested them against NMAP, a network scanner.

8. CONCLUSION

MANETs is an ad-hoc technology which has lots of vulnerabilities and is very insecure. Honeypots have not been implemented on MANETs and the implementation work is still ongoing in this respect. They can be very useful in MANETs to uncover the motive of an attack such as denial-of-service attack or a blackhole attack or data theft in MANETs. The scheme of roaming honeypots can be used in the area of MANETs to find better solution for improving the security of the network. Using roaming technique will help to monitor the MANET network more efficiently as it can cover more area to be monitored and at the same time the honeypot can stay disguised in MANET network very efficiently.

9. FUTURE SCOPE

Future scope for this work is to develop better roaming methodologies in the area of deploying honeypots in MANETs. There is a need to build secure and synchronized communication between honeypots. Key management schemes need to be improved. Election algorithm can be improved for deciding the set of active honeypots and nodes.

10. ACKNOWLEDGEMENT

The authors are thankful to Mr. Aseem Chauhan (Additional President RBEF, Chancellor AUR), Maj. General K. K. Ohri, AVSM (Retd.) Pro Vice Chancellor, AUUP, Lucknow Campus, Prof. S. T. H. Abidi (Director, ASET), Brig. Umesh K. Chopra (Director, AIIT, & Dy. Director, ASET) and Prof. (Dr.) Deepak Arora (HoD, Department of Computer Science) for their cooperation, motivation and suggestive guidance.

11. REFERENCES

[1] Ali Mirzaei *et al*, "Use of Honeypots along with IDS in Cluster-Based MANETs," *American Journal of Scientific Research*, ISSN 2301-2005 Issue 80 November, 2012, pp. 155-163.

[2] Sherif M. Khattab *et al*, "Roaming Honeypots for Mitigating Service-level Denial-of-Service Attacks," Proc. IEEE ICDCS'04, 1063-6927.

[3] HoneySpot: The Wireless Honeypot for Monitoring the Attacker's Activities in Wireless Networks by Raúl Siles, The Spanish Honeynet Project (SHP), http://www.honeynet.org.es

[4] M. Wei and K. Kim, "Intrusion Detection Scheme Using Traffic Prediction for Wireless Industrial Networks," Journal Of Communications and Networks, vol. 14, no. 3, June, 2012.

[5] B. Sun *et al*, "Intrusion Detection System in Mobile Ad-Hoc Networks and Wireless sensor Networks," IEEE Wireless Communications, October, 2007, 1536-1284.

[6] Y. Zhang, W. Lee and Y. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks," ACM Wireless Networks, vol. 9, no. 5, Sept 2003, pp. 361-78

[7] Y. Huang *et al.*, "Cross Feature Analysis for Detecting Ad-Hoc Routing Anomalies," Proc. IEEE ICDCS '03, Providence, Rl, May 2003, pp. 478-87.

[8] Y. Huang and W. Lee, "A Cooperative Intrusion Detection System for Ad-Hoc networks," *ACM SASN '03,* Fairfax, VA, 2003, pp. 135-47.

[9] Shamir, A. (1984). Identity based cryptosystems and signature schemes. In *Proceedings of the CRYPTO'84.*

[10] F. R. Yu and H. Tang, Distributed node selection for threshold key management with intrusion detection in mobile ad-hoc networks, Wireless Network (2010) 16:2169-2178.

[11] J. Li. *et al*. A scalable location service for geographic ad-hoc routing. In *Proc. 6th Annual ACM/IEEE Int'l. Conf. Mobile Comp. Net. (MOBICOM)*, pages 120–130, 2000.

[12] S. Giordano and M. Hamdi. Mobility management: The virtual home region. *Tech. report*, October 1999.

[13] Yu-Chee Tseng *et al,* "Location Awareness in Ad-hoc Wireless Mobile Networks", IEEE, 2001, 0018-9162.

[14] Lance Spitzner, 2003-07-17, "Honeytokens: The Other Honeypot"

[15] Lance Spitzner, "Honeypots: Catching the Insider Threat", Honeypot Technologies Inc., Computer Security Applications Conference, 2003. Proceedings. 19th Annual, pages- 170-179, 2003.

[16] Lance Spitzner, Honeypots: Tracking Hackers, Pearson Education, Inc., 2003.

[17] L. Prema Rajeswari, R. Arockia Xavier Annie, A. Kannan, "Enhanced Intrusion Detection Techniques for Mobile Ad-hoc Networks," ICTES – 2007, Dec 20-22, 2007, pp. 1008-1013.

[18] Suen Yek, "Implementing network defense using deception in a wireless honeypot", syek@student.ecu.edu.au

[19] Liu Dongxia, "An Intrusion Detection System Based on Honeypot Technology", International Conference on Computer Science and Electronics Engineering, IEEE 2012, DOI 10.1109/ICCSEE.2012.158

[20] Rick Schoeneck, "Wireless Honeypot", GIAC Security Essentials Certification (GSEC), Version 1.4b, Option 1, June 8,2003.