ISSN:0975-9646

Ensuring Security in MANET by NRB (NMA Protocol, Roaming Honeypot, Bigdata) Technique

Tarun Varshney, Aishwary Katiyar, [3]Anuj Gupta, Pankaj Sharma

Department Of Information Technology
ABES Engineering College Ghaziabad, India

Abstract—MANETs are the wireless networks of the mobile computing devices with no support of any fixed infrastructure. The mobile nodes use any of the radio technology like Bluetooth, IEEE 802. I I or Hiperlan for directly communicating with each other. The nodes behave as hosts as well as routers. The security challenges in MANET arise due to its dynamic topology, vulnerable wireless link and nomadic environment [1]. Many approaches have been proposed to overcome the same. In this paper, we target at designing an effective and robust technique namely Nimble message authentication protocol and later on using it with roaming honeypots so as to doubly ensure freedom from threats and attacks like man in the middle attack and replay attack, thereby assuring security in MANETs. Finally, big data implementation concepts have been used to continuously record and manage the data generated due to changing locations of roaming honeypot.

I. INTRODUCTION

A Mobile Ad hoc Network (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. People can thus be internetworked in areas without a preexisting communication infrastructure or when the use of such infrastructure requires wireless extension. In MANET, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that are not in the direct communication range use intermediate nodes to communicate with each other. In these two situations, all the nodes that have participated in the communication automatically form a Mobile Ad hoc Network. The mobile nodes within the network can be any moving or fixed-position objects equipped with antennas. MANETs can be used in uncertain situations like disaster relief/rescue operations (Flood, tsunami, earthquake), Education (Virtual classrooms, Conferences), monitoring system (Police raids) etc.

MANETs have the following basic characteristics: Unreliable wireless links between the nodes, dynamically changing topology and absence of infrastructure. It is because of these characteristics that they are more prone to suffer from the security threats, attacks and malicious behavior than the traditional wired networks. Security is difficult to be achieved in MANETs because of vulnerability of links, the limited physical protection of each of the nodes, the sporadic nature of connectivity, dynamic changing topology, and absence of a certification authority and lack of a centralized monitoring or management point [2].

Honeypot is a trap to detect, capture and misguide the intruders who try to attack the system or gain unauthorized access to it. The values of honeypot lies in being attacked. Honeypots can be used to [3]:

- provide extensive study of the attackers.
- provide in-depth analysis of an attack.
- know the motives of an attacker.
- distract the attacker and provide early warning to the system about the attack.
- know the methodology used by the intruder.
- detect the threats, tools used and vulnerabilities the attackers are looking for [4].

Roaming honeypots are a modified version of conventional honeypots. It is a mechanism that allows the location of honeypots to be unpredictable to the attacker, continuously changing and disguised [5]. 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 [6].

The enormous amount of data created every second needs large storage space. The ruining of traditional defensive environments united with attackers' abilities to survive traditional security systems requires us to adopt an intelligence driven security model that is more risk aware, contextual and agile. Intelligence driven security relies on big data analytics. Big data involve both the breadth of sources and the information depth needed for programs to specify risks accurately, to defend against illegal activity and advanced cyber threats. Examples available in literature are astronomy, biological science and research, life sciences, medical records, scientific research, government, natural disaster and resource management, private sector, military surveillance, social networks, web logs, search indexing, mobile phones, sensor networks and telecommunications [7].

II. METHODOLOGY

Talking in terms of MANET, when the number of nodes increases and the Nimble Message Authentication Protocol is used and when the honeypots deployed are roaming honeypots then the information about all the honeypots

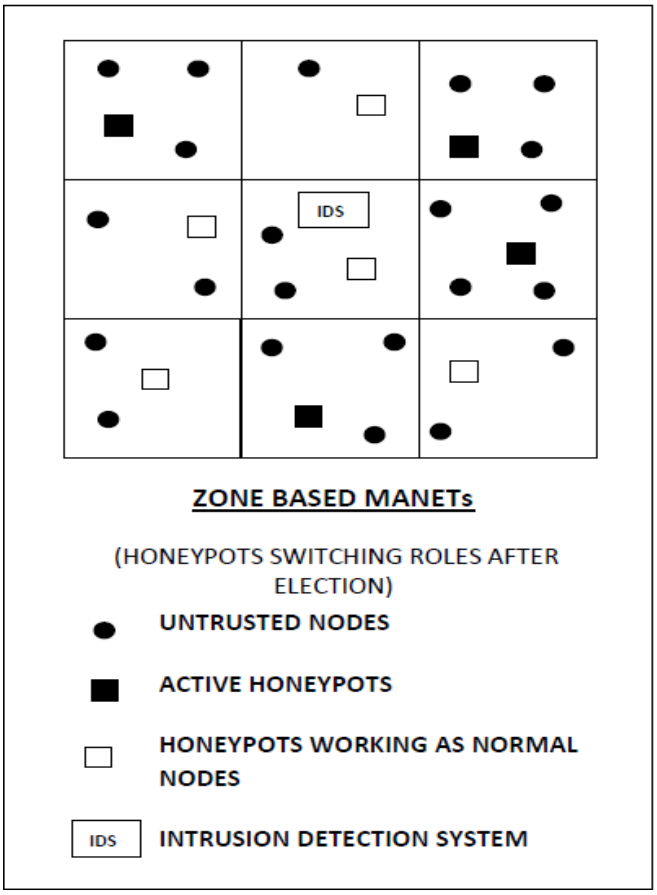
involved and their location information plus the details of all the nodes that form a MANET forms a huge chunk of data, which probably may become unmanageable too. Thus the use of big data implementation methods becomes inevitable. Hadoop is one such Java based framework and heterogeneous open source platform. It is not a replacement for database, warehouse or ETL (Extract, Transform, Load) strategy. Hadoop includes a distributed file system, analytics and data storage platforms and a layer that manages parallel computation, workflow and configuration administration [8].

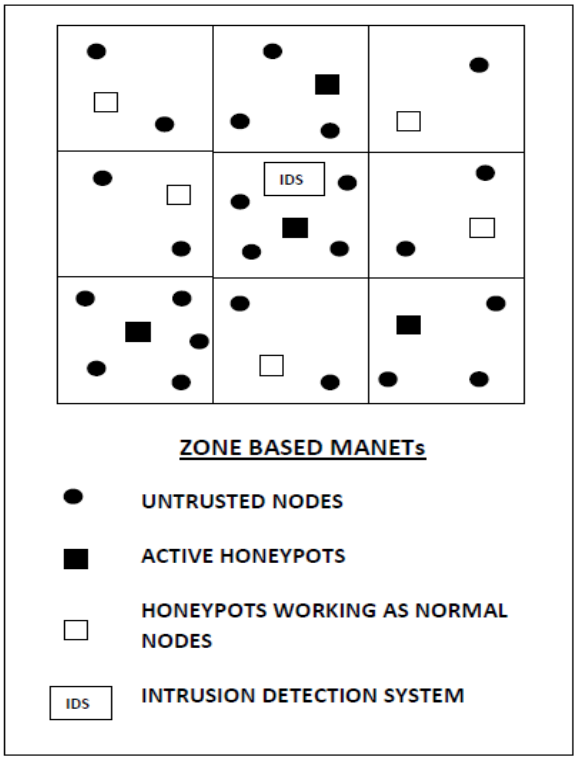
III. ROAMING HONEYPOT SCHEME

For optimal use of honeypots in MANETs, the roaming technique 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 [6].

A. Division Of Network

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).*





B. Selection of Honeypots and Nodes through 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 3.5). 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.

C. 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.

D. 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.

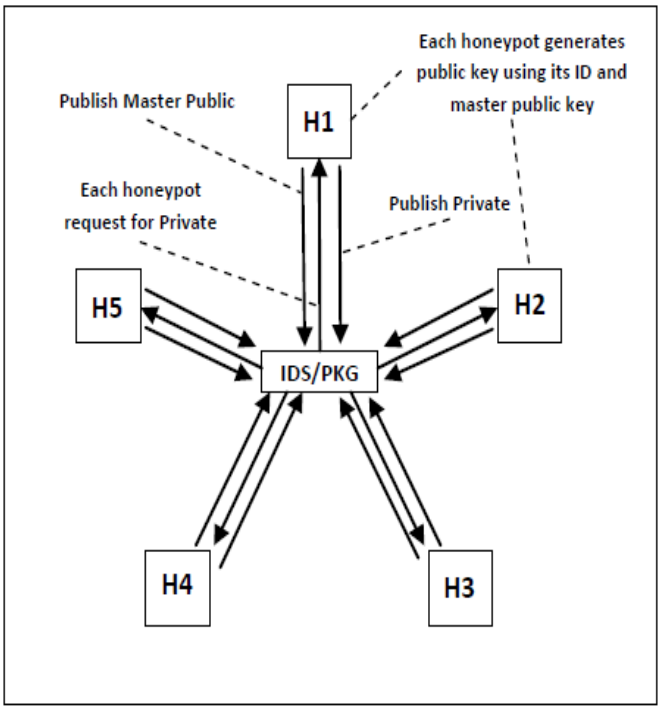
E. Use of ID-based cryptography for secure communication between honeypots

ID based cryptography was first introduced in 1984 by Shamir, A, in "Identity based cryptosystems and signature schemes" [10]. 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 [11]. 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* [11].

F. 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 [12]. 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.



IV. NIMBLE MESSAGE AUTHENTICATION PROTOCOL (NMAP)

This algorithm is a modified version of the Expedite message Authentication protocol [9] which was made originally for VANET (Vehicular Adhoc Network).

The proposed NMAP uses a fast HMAC function and novel key sharing scheme employing probabilistic random key distribution.

2.1 System Model

The system model under consideration consists of the following:

1) A Trusted Authority (TA) which is responsible for providing anonymous certificates and distributing secret keys to all Mobile Nodes in the network.
2) Stationary Nodes (SNs), which are fixed units distributed all over the network. The MNs can communicate securely with the TA.
3) MNs can communicate either with other MNs or with SNs as per the requirement.

For this protocol, we assume some Mobile Nodes (MN) in a MANET to be stationary willingly for the successful implementation of this procedure. These Stationary Nodes are called SNs. These SNs and TA are predetermined by voting by all participating nodes. In case of a tie, the tie breaking is done with help of random selection.

In this paper, we have a prerequisite that each MN is equipped with a safe memory area called Hardware Security Module (HSM).A HSM is a tamper-resistant module used to store the security materials, e.g., secret keys, certificates, etc., of the MN. Also, the HSM in each MN is responsible for performing all the cryptographic

operations such as signing messages, verifying certificates, keys updating, etc. We consider that legitimate MNs cannot collude with the revoked MNs as it is difficult for legitimate MNs to extract their security materials from their HSMs. Finally, we consider that a compromised MN is instantly detected by the TA.

After this we will follow exactly the same steps as given in detail in reference [9].The steps include system Initialization, Message Authentication and Revocation. The OBUs or On Board Units are synonymous to the MNs(Mobile Nodes) in a MANET. The Stationary Nodes(SNs) in MANET are synonymous to the Road Side Units(RSUs) in VANET. The Total Authority in VANET is synonymous to the node chosen by election in a similar fashion like the voting done in section 3.2 of this paper for choosing the active honeypot using ID based Cryptography.

A. Algorithm (1) System initialization

1: Select two generators P,Q that belong to G1 of order q,
2: for i = 1 to l do
3: Select a random number k_i belongs to Z^*_q
4: Set the secret key $K^-_i=k_iQ$ belongs to G1
5: Set the corresponding public key $K_i^+= 1/k_i$ P belongs to G1
6: end for
7: Select an initial secret key Kg belongs to G2 (to be shared between all the non-revoked MNs)
8: Select a master secret key s belongs to Z_q^*
9: Set the corresponding public key $P_o = sP$
10: Choose hash functions H : {0 , 1}* ->G1 and h : {0,1}* -> Zq^*
11: Select a secret value v belongs to Zq and set $v_o = v$
12: for i =1, j do (to obtain a set V of hash chain values)
13: Set vi =h(vi - 1)
14: end for
15: for all MN_u in the network, TA do
16: for i =1, m do
17: Select a random number a belongs to [1,l]
18: Upload the secret key K_a^- = kaQ and the corresponding public key K_a^+ = (1/ka)P in HSMu which is the HSM embedded in MNu
19: end for
20: Generate a set of anonymous certificates CERTu = $\{cert^i_u$ (PIDi , PK^i_u , $sig_{TA}(PID^i_u||PK^i_u)) \mid 1 <= I <= C \}$ (for privacy-preserving authentication)
21: Upload CERTu in HSMu of MNu
22: end for
23: Announce H, h, P, Q, and P_O to all the MNs

PK^i_u = i^{th} public key for MN
SK^i_u = Corresonding secret key
PID^i_u = i^{th} pseudoIdentity for MN such that only TA can associate PID^i_u to real identity of MN
$sig_{TA}(PID^i_u||PK^i_u)$ = the TA signature on concatenation of PID^i_u with PK^i_u
C= total number of certificates loaded in MN.

B. Message Signing

Before any MNu broadcasts a message M, it calculates its revocation check REVcheck as REVcheck = $HMAC(Kg,PIDu ||Tstamp)^2$ where Tstamp is the current time stamp, and HMAC(Kg,PIDu ||Tstamp) is the hash message authentication
code on the concatenation of PIDu and Tstamp using the secret key Kg. Then, MNu broadcasts
(M||Tstamp||certu(PIDu , PKu, sigTA (PIDu||PKu))||sigu(M||Tstamp)||REVcheck);
where sigu(MkTstamp) is the signature of MNu on the concatenation of the message M and Tstamp.

C. Message Verification

Any MNu receiving the message (M||Tstamp ||certu(PIDu, PKu, sigTA(PIDu ||PKu))||sigu(M||Tstamp)||REVcheck) can
erify it by executing Algorithm 2.

D. Algorithm (2) Message verification

Require: (M||Tstamp||certu(PIDu , PKu , sigTA (PIDu|| PKu))||sigu(M||Tstamp)||REVcheck) and Kg
1: Check the validity of Tstamp
2: if invalid then
3: Drop the message
4: else
5: Check REVcheck = HMAC(Kg, PIDu||Tstamp)
6: if invalid then
7: Drop the message
8: else
9: Verify the TA signature on certMNu
10: if invalid then
11: Drop the message
12: else
13: Verify the signature sigu(M||Tstamp) using MNu public key (PKu)
14: if invalid then
15: Drop the message
16: else
17: Process the message
18: end if
19: end if
20: end if
21: end if

V. BIG DATA

To successfully analyze and use the huge lot of data processed(information) via the use of roaming honeypots and NMAP protocol, we need some way to quickly process and extract useful information from this data. It is then when Big data and Hadoop come to our rescue. Although, typical programming language constructs or language algorithms have not been given to promote generality, the big data analysis methods prove useful when large quantity of dat is to be processed in short time.

A. Knowledge Discovery from Big Data

Knowledge Discovery from Data (KDD) entitle as some operations designed to get information from complicated data sets [13]. Reference [14] outlines the KDD at nine steps:

1) Application domain prior to information and defining purpose of process from customer's perspective.

2) Generate subset data point for knowledge discovery.

3) Removing noise, handling missing data fields, collecting required information to model and calculating time information and known changes.

4) Finding useful properties to present data depending on purpose of job.

5) Mapping purposes to a particular data mining methods.

6) Choose data mining algorithm and method for searching data patterns.

7) Researching patterns in expressional form.

8) Returning any steps 1 through 7 for iterations also this step can include visualization of patterns.

9) Using information directly, combining information into another system or simply enlisting and reporting.

Reference [13] analyzes knowledge discovery from big data in three principles using Hadoop. These are:
1) KDD includes a variety of analysis methods as distributed programming, pattern recognition, data mining, natural language processing, sentiment analysis, statistical and visual analysis and human computer interaction. Therefore architecture must support various methods and analysis techniques.

 Statistical analysis interested in summarizing massive datasets, understanding data and defining models for prediction.

 Data mining correlate with discovering useful models in massive data sets by itself, machine learning combine with data mining and statistical methods enabling machines to understand datasets.

 Visual analysis is developing area in which large datasets are serviced to users in challenging ways will be able to understand relationships.

2) A comprehensive KDD architecture must procure to keep and operate process line.
 Preparation of data and batch analytics are made, for proper troubleshooting with errors, missing values and unusable format.

 Processing structured and semi structured data

3) It is cardinal that making results accessible and fool proof. For this reason following approaches are used to overcome this issue.

 Using open source and popular standards

 Use WEB based architectures

 Publicly available results

VI. CONCLUSION

Use of roaming honeypots, then NMAP protocol and then finally using big data are great insights provided as guidelines on such a lot of future research can be based. It is a successful method because it effectively combines two security mechanisms and also couples big data analysis requirements with it. Thereby paving a way for secure communication between nodes in MANET. Attacks like the replay attack and Man in the Middle attack will be intercepted to quite a large degree because of double security provided by a combination of roaming honeypots and Nimble Message authentication Protocol, both of which have been successfully implemented in their respective references[6][9].

REFERENCES

[1] Security Issues in MANET: A Review. Mahakal Singh Chandel, Arjun Institute of Advaced Studies and Research Centre, Indore, India. Rashid Sheikh, Durgesh Kumar Mishra, Acropolis Institute of Technology and Research, Indore, India,2010 IEEE.

[2] Security Architecture for MANET and It's Application in m-Governance, Baljeet Kaur, Bharati Vidyapeeth Deemed University, Pune. Institute of Management and Entrepreneurship Development. 2013 International Conference on Communication Systems and Network Technologies.

[3] T. H. project, "Know your enemy," July 2000. [Online]. Available: http://project.honeynet.org/papers

[4] Locating the Attacker of Wormhole Attack by Using the Honeypot.T Divya Sai Keerthi and Pallapa Venkataram. *Electrical Communication Engineering Department, Indian Institute of Science, Bangalore, India.* 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications.

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

[6] Roaming Honeypots along with IDS in Mobile Ad-Hoc Networks. Sabah Shamsh, Vandana Dubey. Department of Computer Science, Amity University Lucknow, India. *International Journal of Computer Applications (0975 – 8887) Volume 69– No.23, May 2013*

[7] http://en.wikipedia.org/wiki/Big_data , last access 11.03.2013

[8] Big Data: A Review. Seref SAGIROGLU and Duygu SINANC, Gazi University. Department of Computer Engineering, Faculty of Engineering, Ankara, Turkey. IEEE, 2013.

[9] EMAP: Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks. Albert Wasef and Xuemin (Sherman) Shen, IEEE, Fellow

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

[11] 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.

[12] 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.

[13] E. Begoli and J. Horey, "Design Principles for Effective Knowledge Discovery from Big Data", Software Architecture (WICSA) and European Conference on Software Architecture (ECSA) Joint Working IEEE/IFIP Conference on, Helsinki, August 2012

[14] U. Fayyad, G. Piatetsky-Shapiro and P. Smyth, "From Data Mining to Knowledge Discovery in Databases", American Association for Artificial Intelligence, AI Magazine, Fall 1996, pp. 37- 54