RESEARCHERID
THOMSON REUTERS

[Ahmed, 5(8): August 2018]
DOI- 10.5281/zenodo.1342512

ISSN 2348 – 8034
Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

REDUCING THE NETWORK OVERHEAD BY IMPLEMENTING DISTRIBUTED KEY MECHANISM IN MANETS

Mohammed Aziz Ahmed*[1], Mohammed Sirajuddin[2] & Nazia Kouser[3]

[*1]Department of CSE, Research Scholar, Shri Venkateshwara University, Gajraula, Amroha (UP) India
[2]Department of CSE, Visiting Professor, Shri Venkateshwara University, Gajraula, Amroha (UP) India
[3]Department of ECE, Research Scholar, Shri Venkateshwara University, Gajraula, Amroha (UP) India

ABSTRACT

In the wireless sensor networks, the Mobile Ad hoc Networks (MANETs) is a type of networks. The difference between wireless network and MANETs is, in the wireless network the nodes are stable and in MANETs no one node is stable which means these are mobile nodes. Generally, any network hasinformation security breaches.The closing purpose of the security answers for MANETs is to provide protection offerings, which includes authentication, confidentiality, integrity, anonymity, and availability, to cellular user. In order to acquire this goal, the security solution required to provide complete protection spanning the entire protocol stack.And different type of attacks is providing violations to the network user's data. Hence, in this paper we are focusing on the Mobile Ad Hoc Networking (MANET) and Routing overheads for MANETs. And also we will provide the key mechanism to avoid the security violations or breaches.

Keywords: *MANETs, Seurity Breaches, Attacks, Integrity, Anonymity.*

I. INTRODUCTION

MANET is dynamically establishing cellular nodes networks and not using a fixed infrastructure. Each mobile node is ready with wi-fi transmitter and a receiver with a suitable antenna. Nodes in cell ad hoc networks move freely in the network and they are able to organize themselves in a random way. The crucial zone of ad hoc network is routing protocols [5] because network topologies hold on changing because of the motion of the nodes. All the network related sports like discovering of topology and transport of packets is achieved by way of the nodes itself. The nodes communicate over wireless hyperlinks; they need to compete with the results of radio verbal exchange, such as noise and interference. In Manet the links typically have less bandwidth than a stressed out network. Each node in a wireless ad hoc network features as a number as well as a router. The control of the network is shared among all the nodes of the network.

Since MANET's have special characteristics[1], [8], [9] there are a few crucial metrics in MANET safety which can be important in all security approaches; we call them "Security Parameters". Being unaware of these parameters might also motive a security method vain in MANET. Each security method should be aware of safety parameters All mechanisms proposed for protection elements, must be aware of these parameters and don now not push aside them; otherwise they will be useless in MANET.

The essential vulnerability of MANETs comes from their open peer-to-peer architecture. Unlike stressed networks which have dedicated routers, every cellular node in an ad hoc network may also characteristic as a router and forward packets for different nodes. The wireless channel is obtainable to both valid network users and malicious attackers. As a end result, there is no clean line of protection in MANETs from the security layout angle. The boundary that separates the internal network from the outside international turns into blurred. There is not any properly defined place/infrastructure where we can also installation a single safety solution. Moreover, portable devices, as well as the system security data they store, are vulnerable to compromises or physical seize, in particular low-stop gadgets with susceptible safety. [3], [10] Attackers may additionally sneak into the network through those

subverted nodes, which pose the weakest hyperlink and incur a domino effect of safety breaches in the gadget. The stringent useful resource constraints in MANETs constitute every other nontrivial mission to safety layout. The wireless channel is bandwidth-restricted and shared among a couple of networking entities. The computation functionality of a cell node is likewise constrained. For example, some low-stop gadgets, including PDAs, can rarely perform computation-in depth tasks like uneven cryptographic computation. Because mobile gadgets are usually powered by batteries, they'll have very confined energy assets. The wireless medium and node mobility poses a long way extra dynamics in MANETs in comparison to the stressed networks. The network topology is relatively dynamic as nodes often are a part of or depart the network, and roam in the network on their personal will. The wireless channel is also problem to interferences and mistakes, displaying risky traits in terms of bandwidth and delay. Despite such dynamics, cell customers may additionally request for anytime, anywhere safety offerings as they move from one region to another. The above characteristics of MANETs surely make a case for constructing multifence protection answers that achieve both large protection and desirable network overall performance.

II. RELATED WORK

AsifShabbir et al [2] addressed each and each aspect of the MANET this is concerned with the safety in any manner at any quantity. They started from the scratch; we discussed the architecture of MANET, vulnerabilities of the MANET, distinctive safety threats and even exclusive sorts of protection assaults of their study. Non-solid architecture of MANETs and wi-fi vulnerabilities helped us to apprehend, why the MANETs are smooth to attack. Layer smart network assaults and their proposed answers enlightened us to apprehend the way of movement and execution plan of different network assaults. From the whole scene one element is crystal clear that MANETs will pass at the manner within the identical fashion with none important change. Wireless is their natural best friend as a communication medium; there's no substitution or opportunity of wireless medium. These matters will persist at the least in close to destiny unless the emergence of any new era. Even though there may be the discovery on any substitution, it'll take long to exchange to that precise generation. At present we ought to receive the MANETs and wireless vulnerabilities as a good evil. We could make effort to improve the matters by way of keeping in mind these vulnerabilities. For a second if we suppose definitely, in reality we are blessed with aoutstandingroom, from research point of view because of those vulnerabilities of the MANET and wi-fi medium. A lot of studies paintings has been achieved through the researchers however nevertheless there are lots to do. Network security is a dynamic problem. New and new attacks are getting delivered. So the regular efforts are required to make the MANET more and more relaxed. There is lots of research scope within the area of relaxed routing. Intrusion detection and its recovery is any other research hot spot for the network protection researchers. Most of the intrusion detection structures and strategies appearance very stunning and convincing on researches but still implemented studies design is expecting the researchers in positive areas of network protection. There is want to enforce, evaluate and enhance these intrusion detection systems practically.

All sorts of attacks to which MANETs are vulnerable are being presented by Ms.Supriya and Mrs.ManjuKhari [3]. A short assessment of problems required to be taken into consideration for designing at ease routing protocols is also supplied closer to the cease of this paper. However, MANETs are in a untimely state and affords a extensive scope of research. To utilize the dynamicity and robustness of those networks efficiently and reliably, it's far required to recognize its secure needs.

III. PROPOSED WORK

Overview of Proposed System:
In existing work attacker node steal identity of genuine node and authenticate himself with other node in the network, when any source sends its data to attacker node then it drop packets instead of sending to destination.

In this paper to avoid breaches (attack or violation) and to provide security to MANET we can use secure distributed key mechanism using node x and y locations and random values from additional node called Security Center.

A. Security Services and Challenges in MANETs

Availability:
In this service, each legal node has to have got right of entry to all facts and offerings in the network. Availability undertaking arises due to MANET's dynamic topology and its open boundary. Accessing time, that is the time needed for a node to get right of entry to the network services or statistics is important, due to the fact time is one of the protection parameters.

Authentication:
The goal of this service is to offer trustable communications between two different nodes. When a node receives packets from a source, it must be in no question about identity of the supply node. To provide this service it's far the use of certifications; key distribution and key management are challengeable [4]

Data confidentially:
According to this service, each node ought to have get entry to unique offerings that it has the permission to get right of entry to. Most of services that are furnished by means of facts confidentially use encryption strategies but in MANET there is no primary management, key distribution confronted masses of demanding situations and in a few instances impractical.

Integrity:
According to integrity security service, simplest legal nodes can create, edit or delete packets. As an instance, Man-In-The-Middle attack is towards this provider. In this attack the attacker captures all packets after which removes or modifies them. Non-

Repudiation:
By using this service, neither source nor destination can repudiate their actions or information. It means if a node 1 receives a packet from node 2, and sends a reply to node 2 can't repudiate the packet that it's been dispatched.

B. Distributed Key Mechanism in MANETs

Cryptographic Key technology and different strategies are mounted to encrypt and authenticate the messages which might be transferred through numerous wireless networks [4], [6], [7]. The applications that make use of the wireless infrastructure to switch the message had been accelerated over beyond years. Therefore, it's far necessary to challenge on the security troubles of wireless networks. The extensively used wireless network is MANET. Several Cryptographic strategies had been proposed to generate key which could authenticate the MANET to make certain network protection. The security of this network completely relies upon at the mode of key applied to a selected network. Using a single shared key for the entire network that runs greater range of programs isn't relaxed. Therefore, pair-sensible key era the usage of a number of the famous cryptographic techniques may be used to authenticate the network from unauthorized user.

C. Proposed System Work flow

1) **Initialization steps:** In this step Security Center will generate random value and distribute it to all nodes in the network.
2) **Key Generation:** In this step all nodes identify its location (x and y position) and perform XOR operation between location value and random value received from Security Center
3) **Key Share:** In this step all nodes share their generated keys with all their neighbors.
4) **Key verification:** In this steps if any source receives reply from neighbor then it will check its new received key with all keys share earlier. If both keys match then verification will be successful.

Key Verification Algorithm:
Input: source, destination
Output:genuine_neighbor
Initialize keys with security center

ISSN 2348 – 8034
Impact Factor- 5.070

```
For(i=0 to all nodes){
Identify location
Set key(i) = location ^ key;
  }
Find neighbors of source
If(neighbor(keys) == existingkey){
Start packet transmission
}else {
Look second genuine neighbor
Start packet transmission
}
```

5) **Data Encryption:** In this step source encrypt message with its key
6) **Data Decryption:** In this step destination decrypt message by using keys which share earlier.

D. Hierarchical MANETs for Military Use

Hierarchical MANETs, namely, the UAVMBN networks and in a UAV-MBN network, there are three node levels:

1. Ground MANETs
2. MBN
3. UAV

Nodes at each level have different communication and computation abilities, as follows from fig1.

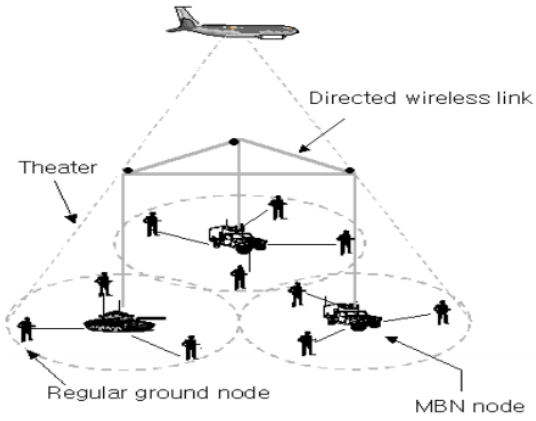


Fig1. Hierarchical MANETs I Military

Ground MANET

It consists of both everyday floor nodes and MBN nodes. Regular ground nodes are typically soldiers/retailers geared up with communication and computation restrained devices. They speak via bandwidth limited brief-variety broadcast wi-fi channel.

Ground Mobile Backbone Network (MBN)

MBN nodes are special devices consisting of tanks and employees services. They have extra full-size centers than everyday floor nodes. In precise, they've more verbal exchange and computation power. MBN nodes can establish direct wi-fi hyperlinks for verbal exchange amongst themselves. Regular ground nodes and MBN nodes form an awesome-MANET with clustered hierarchy wherein MBN nodes act as cluster-heads.

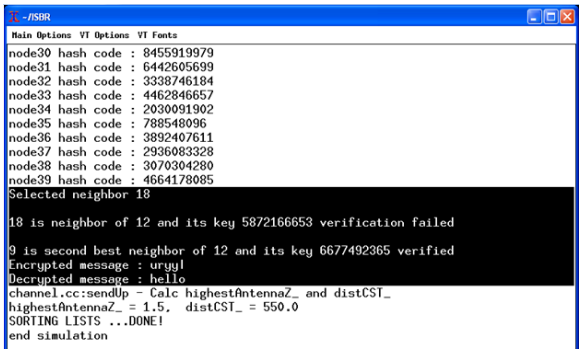
Unmanned Aerial Vehicles (UAVs)

Each UAV leads a single-area theater. With the assist of phased-array antennas, a UAV can provide the shared beam to its MBN nodes to keep line-of-sight connectivity for one place of operations under.

The application of ad hoc networks in a military environment is in particular appealing because of their lack of infrastructure and self-organizing nature. Consider traditional networks that depend upon infrastructure which include base stations, the infrastructure introduces factors of vulnerability which can be attacked and, if eliminated, dismantle the operation of the whole community. In struggle field eventualities, strong and warranted verbal exchange is essential, with probably deadly effects if compromised. Ad hoc networks can continue to exist even within the event of nodes becoming disconnected due to bad wireless connectivity, nodes being compromised or switched off, nodes transferring out of range, node being damaged at some point of bodily assault on customers, or nodes failing due to malfunction or battery depletion. Applications together with sensor networks, positional network structures and tactical ad hoc networks will stay some of the driving forces behind ad hoc network development. The primary characteristic of navy-type MANETs is using an offline authority. In authority-based MANETs, nodes proportion pre-set up relationships initialized through the offline authority. The presence or absence of a priori safety relationships has an essential impact at the layout method of key control schemes for MANETs.

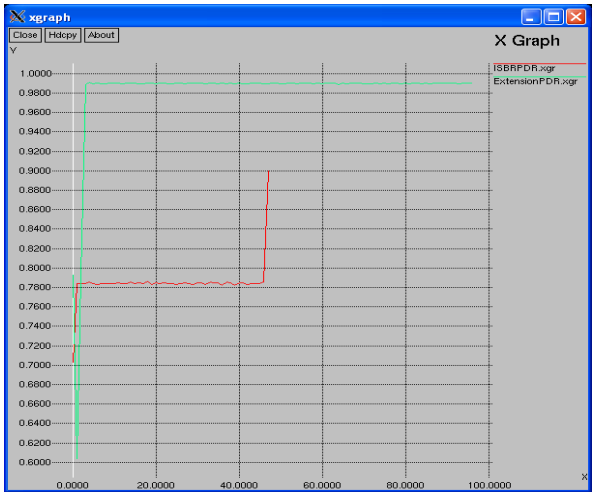
IV. EXPERIMENTAL RESULTS

In this experiment we used NS-2 simulator to avoid the security breaches of MANETs. We are simulating propose technique called ISBR and 40 is total no of nodes and 12 is source node and 33 is destination node and 0 means all nodes are genuine node. As we are doing simulation we only need to act as normal and attacker.



Here, while sending data from source to destination, if key verification may fail then source will not communicate with the neighbor. And immediately, the communication stop in the network due to key verification failed and we can resume this communication by using second best genuine neighbor for the source and due to this technique network Packet Delivery Ratio will increase.

ISSN 2348 – 8034
Impact Factor- 5.070



We observed that the proposed work can reduce the network overhead.

V. CONCLUSION

In this paper we focused on the information security breaches in MANETs. To avoid the security breaches in MANETs, we proposed distributed key mechanism in this paper. The proposed key mechanism used XOR operation to verify the key of network nodes. By extending the proposed work, even though key verification may fail, sender node can select the best neighbor node in the network.

REFERENCES

1. *TripathiLalit Kumar and Dr. KanojiaSindhuben, "MANET: Security and Challenges", International Journal of Computer Science and Information Technologies, Vol. 7 (5) , 2016, 2381-2384*
2. *AsifShabbir, Fayyaz Khalid, Syed MuqsitShaheed, Jalil Abbas and M. Zia-Ul-Haq, "Security: A Core Issue in Mobile Ad hoc Networks", Journal of Computer and Communications, 2015, 3, 41-66*
3. *Ms.Supriya and Mrs.ManjuKhari, "MANET Security Breaches : Threat To A Secure Communication Platform", International Journal on AdHoc Networking Systems (IJANS) Vol. 2, No. 2, April 2012*
4. *Abu TahaZamani and Syed Zubair, "Key Management Scheme in Mobile Ad Hoc Networks"International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-3, Issue-4)*

5. *Manel Guerrero Zapata and N. Asokan, "Securing Ad hoc Routing Protocols"*
6. *N. Vimala and Dr. R. Balasubramaniam, "Distributed Key Management Scheme for Mobile Ad-Hoc Network-A Survey", Global Journal of Computer Science and Technology Vol. 10 Issue 2 (Ver 1.0), April 2010*
7. *Kyung Hyune Rhee, Young Ho Park, and Gene Tsudik, "An Architecture for Key Management in HierarchicalMobile Ad-hoc Networks", JOURNAL OF COMMUNICATIONS AND NETWORKS, VOL. 6, NO. 2, JUNE 2004 1*
8. *Florian, D. (2008) Security Concepts for Robust and Highly Mobile Ad-hoc Networks. April.*

E. *Gu et al., "Hierarchical routing for multi-layer ad-hoc wireless networks with UAVs," in Proc. IEEE MILCOM'2000, 2000, pp. 310–314.*

9. *D. Gu et al., "UAV-aided intelligent routing for ad-hoc wireless network in single-area theater," in Proc. IEEE WCNC'2000, 2000, pp*