National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Army Security Communication Network - An Review on Inter Tactical Mobile Ad Hoc Network Routing Protocol

Goutham S Tantri, Manjunatha M J
UG Scholar, Department of Electronics and communication, Jawaharlal Nehru National College,
Shivammoga, Karnataka, India

ABSTRACT

Mission-critical military operations with dismounted soldiers are frequently characterized by high battlefield dynamics. In such scenarios a mobility model can manage soldiers' movements dynamically especially under enemy attacks. MOBILE armies need mobile communications. Those communications, though, must be secure—and not just from eavesdropping. They also need to be uninterruptible, The battlefield where these equipment are deployed includes a majority of coalition communication. Each group on the battleground may communicate with other members of the coalition and establish inter-MANETs links. Operational communications tend to provide tactical ad hoc networks some capacities. There is a better broadband radio in UHF band (ex: NATO - 225-400 MHz) and some heterogeneous services such as voice or video are provided. Several Network-layer protocols have been proposed in order to handle inter-domain routing for tactical MANETs. One key factor is the much more dynamic pattern of participation of individual nodes in a MANET. Today's operations can be much more ad hoc in terms of the use of unmanned vehicles, or airborne assets .This MANET communication networking comes handy in relocating operations, rescue operation and can even be applied in daily civilian usage

Keywords : Self-Organized Behavior, Mobility Models, Ad hoc Networks, Group mobility, Dismounted soldiers, Battlefield, MANET.

I. INTRODUCTION

Recently, the army has been interested in developing new skills and competencies such as making soldiers more connected in the battlefield based on modern electronic communication equipment and computer technologies by using mobile wireless ad hoc networks (MANETs) . Mobile ad hoc networks are useful in situations where there are no network infrastructures available and when there is a need for people to communicate using mobile devices. Since MANETS are based on wireless transmission, a secured way of message transmission is important to protect the privacy of the data. An insecure ad-hoc network at the edge of an existing communication infrastructure may potentially cause the entire network to become vulnerable to security breaches. The intrinsic nature of wireless ad hoc networks makes them very vulnerable to attacks ranging from passive spying to active interference. In mobile ad hoc networks, there is no central administration to take care of detection and prevention of anomalies. However, most of the existing key management schemes are not feasible in ad hoc networks because public key infrastructures with a centralized certification authority are hard and cost ineffective to deploy. Consequently mobile devices identities or their intentions cannot be predetermined or verified. Therefore nodes have to cooperate for the integrity of the operation of the network. However, nodes may refuse to cooperate by not forwarding packets for others for selfish reasons and not want to exhaust their resources. Various other factors make the task of secure communication in ad hoc wireless networks difficulties which includes the mobility of the nodes, a promiscuous mode of operation, limited processing power, and limited availability of resources such as battery power, bandwidth and memory. Attacks on ad hoc are classified into non disruptive passive attacks and disruptive active attacks. The active attacks are further classified into external attacks and internal one. External attacks are carried out by nodes that do not belong to network and can be prevented by firewalls and encryption techniques. Internal attacks are from internal nodes which are actually authorized nodes and part of the network , hence it is difficult to identify them. Lot of works had been done in the area of identifying and removal of adversaries in the network. The SMT protocol safeguards pair wise communication across an unknown frequently changing network, possibly in the presence of adversaries that may exhibit arbitrary behavior. Instead of transmitting in single path, the message will be transmitted in multiple paths to ensure reliability. Considering the benefits over the overhead involved in utilizing the multiple paths are increased security, reliability and reduced congestion that is mostly needed for MANETs in military.SMT protocol provides security based on the security association between the end nodes. It is not able to overcome the compromised nodes attacks. And to improve the security and reliability of data transmission in mobile ad hoc networks by providing secured routes. The Byzantine faults are identified and those links will be avoided in the data transmission phase. The current topological information will be gathered based on the network behavior such as transmission time, Probability of lost packets and correctly received – acknowledged packets and a threshold is set which is used in binary search probing.

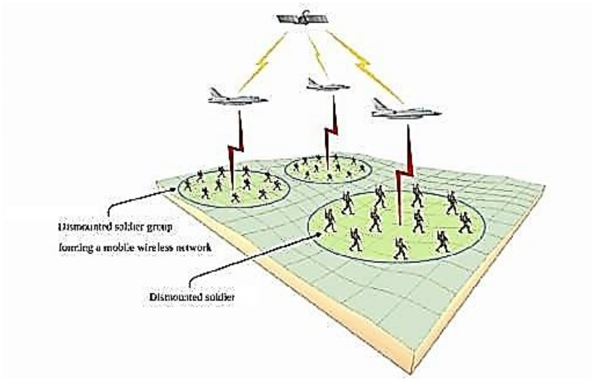


Fig. 1. Illustration of dismounted soldier group in military modern communications infrastructure.

History

We can characterized the life cycle of mobile ad hoc network into first, second and third generation. Present ad hoc network are considered the third generation .The first generation of ad hoc network can be traced back to 1970's. In 1970's, these are called Packet Radio Network (PRNET) .The Defence Advanced Research Project Agency (DARPA) initiated research of using packet- switched radio communication to provide reliable communication between computers and urbanized PRNET. Basically PRNET uses the combination of Areal Location of Hazardous Atmospheres (ALOHA) and Carrier Sense Multiple Access (CSMA) for multiple access and distance vector routing .The PRNET is then evolved into the Survivable Adaptive Radio Network (SURAN) in the early 1980's. SURAN provides some benefits by improving the radio performance (making them smaller, cheaper and power thrifty). This SURAN also provides resilience to electronic attacks.

Around the same time, United State Department of Defence (DOD) continued funding for programs such Globe Mobile Information System (GloMo) and Near Term Digital Radio (NTDR). GloMo make use of CSMA/CA and TDMA molds, and provides self-organizing and self-healing network (i.e. ATM over wireless, Satellite Communication Network). The NTDR make use of clustering and link state routing and organized an ad hoc network. NTDR is worn by

US Army. This is the only "real" ad hoc network in use. By the growing interest in the ad hoc networks, a various other great developments takes place in 1990's.

The functioning group of MANET is born in Internet Engineering Task Force (IETF) who worked to standardized routing protocols for MANET and gives rise to the development of various mobile devices like PDA's , palmtops, notebooks, etc . Meanwhile the Development of Standard IEEE 802.11 (i.e. WLAN's) benefited the ad hoc network. Some other standards are also developed that provide benefits to the MANET like Bluetooth and HIPERLAN.

II. METHODS AND MATERIAL

Manet Challenges

Unless the variety of applications and the long history of mobile ad hoc network, there are still some issues and design challenges that we have to overcome . This is the reason MANET is one of the elementary research field. MANET is a wireless network of mobile nodes, its a self organized network. Every device can communicate with every other device i.e. it is also multi hop network.

As it is a wireless network it inherits the traditional problem of wireless networking:

- The channel is unprotected from outside signal.
- The wireless media is unreliable as compared to the wired media.
- Hidden terminal and expose terminal phenomenon may occur.
- The channel has time varying and asymmetric propagation properties .

Along with these problems there are some other challenges and complexities MANET facing they are:

- The scalability is required in MANET as it is used in military communications, because the network grows according to the need , so each mobile device must be capable to handle the intensification of network and to accomplish the task.
- MANET is a infrastructure less network, there is no central administration. Each device can communicate with every other device, hence it becomes difficult to detect and manage the faults. In MANET, the mobile devices can move randomly. The use of this dynamic topology results in route changes, frequent network partitions and possibly packet losses .
- Each node in the network is autonomous; hence have the equipment for radio interface with different transmission/ receiving capabilities these results in asymmetric links. MANET uses no router in between.
- In network every node acts as a router and can forward packets of data to other nodes inorder to provide information partaking among the mobile nodes. Difficult chore to implement ad hoc addressing scheme, the MAC address of the device is used in the stand alone ad hoc network. However every application is based on TCP/IP and UDP/IP.

Areas Possible Scenarios

- **Military Scenarios** MANET supports tactical network for military communications and automated battle fields.
- **Rescue Operations** It provides Disaster recovery, means replacement of fixed infrastructure network in case of environmental disaster.
- **Data Networks** MANET provides support to the network for the exchange of data between mobile devices.
- **Device Networks** Device Networks supports the wireless connections between various mobile devices so that they can communicate.
- **Free Internet Connection Sharing** It also allow us

to share the internet with other mobile devices.

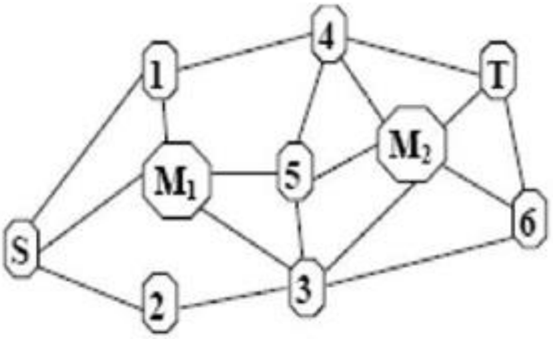
- **Sensor Network** It consist of devices that have capability of sensing, computation and wireless networking . Wireless sensor network combines the power of all three of them, like smoke detectors, electricity, gas and water meters

III. RESULTS AND DISCUSSION

A. Secure Communication Ways

Secure message Transmission

A.Secured Route Discovery by SMT Secured routes are provided by establishing an End-to-End security association between the source and the destination. This scheme won't consider the intermediate nodes that may exhibit arbitrary and malicious behavior. The source node S and destination node T negotiate a shared secret key- KS, T with the knowledge of each other's public key. A pair of identifiers - query sequence number and query identifier is generated and used for the construction of the route request packet. The identifiers along with source and destination and KS,T are used for the calculation of Message Authentication Code (MAC). The identities of the traversed intermediate nodes are added in the route request packet. The route request is denoted as a list {Q S, T: n1, n2 …nk}.The route reply is denoted as a list {RS, T : n1,n2 …nk}.



Sample Topology with two malicious nodes M1, M2

Figure 2

Security Provided by SMT under Various Attacks

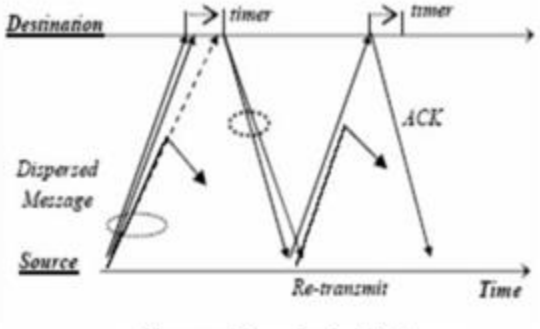
1) Fake Reply: If M1 receives the request by S and reply a fake route to S, that false reply will be discarded by the source since M1 doesn't know KS,T and not able to produce a valid MAC.

2) Tampering Route Reply: If the malicious nodes M1 or M2 changes the route reply send by T, S will discard it as the modified reply won't integrate with the expected MAC of T.

3) Resource Consumption Attack: If the adversaries want to exhaust the network resources then they will replay the requests. On receiving the replayed requests, the nodes will drop the requests based on query identifiers.

4) Fabricated Route Requests: Malicious nodes after observing for some time the requests generated by source, it will fabricate several queries with subsequent query identifiers. The goal is the intermediate nodes will store this numbers and drop out the legitimate requests sent by the source. This type of attack cannot be prevented by SMT.

5) Spoofing Attack: The nodes M1 and M2 may spoof an IP address and participate in the route requests. This attack cannot be identified and they can hide their location by masking.



Message Dispersion in SMT

Figure 3

Secured Data Communication of SMT

6) Active Path Sets(APS) and Message Transmission: A set of diverse, node disjoint multiple paths are selected by applying secured route discovery protocol. The set of paths used for current data transmission are known as Active Path Sets. The message is dispersed based on Robin's algorithm and is transmitted in multiple paths by dispersing it into pieces and after encoding. Redundancy ensures successful reconstruction of data even if some loss occurs due to malicious nodes or breakage of routes. Figure 2. Message Dispersion in SMT

7) Robust Feedback Mechanism: Each dispersed piece is transmitted in different route and carries a Message Authentication Code and by that the integrity of the message and authenticity of the source is verified. After validation, the destination acknowledges every successful receipt. The feedback mechanism is also cryptographically protected and dispersed.

8) APS Adaptation: Successful receipt of ACKS indicates operational routes while missing ACK implies that the route is either broken or compromised. The paths are rated based on short

term and long term rating. The routes are selected or discarded based on their rates. D. Byzantine Attacks Here, a compromised intermediate node or a set of compromised intermediate nodes works in collusion and carries out attacks such as creating routing loops, routing packets on non optimal paths, and selectively dropping packets. Byzantine failures are hard to detect. The network would seem to be operating normally in the viewpoint of nodes, though it may actually be exhibiting Byzantine behaviour . As discussed above, SMT is able to avoid only the rooting loops attacks caused by colluding nodes Secure Message Transmission movement in dynamic environment with near proximity is needed.

B. Byzantine Fault Detection

The detection scheme is based on using acknowledgements of the data packets. The destination has to return an acknowledgement to the source for every successfully received data packet. Timeouts are set for receiving the valid acknowledgements. The delay in receipt may be due to either malicious or non malicious causes. A threshold is set to a tolerable loss rate. A fault is defined as a loss rate greater than or equal to the threshold. The source keeps track of the number of recent losses. If the number of recent losses is greater than the acceptable threshold then a fault is registered and a binary search starts between the source and the destination in order to find the faulty link. The source controls the search by specifying a list of intermediate nodes on data packets. Each node in the list in addition to the destination must send an acknowledgement to the source. The list of nodes those have to send acknowledgements are known as probe nodes. Since the list of probed nodes is specified on legitimate traffic, an adversary is unable to drop traffic without also dropping the list of probed nodes and finally being detected. This scheme is able to detect all types of Byzantine attacks including network overlay attacks. Shared keys are used between the source and the probed nodes .This can be done by on demand Diffie-Hellmann key exchange algorithm. This key mechanism can be integrated into the route discovery protocol.

C. Binary Search Probing

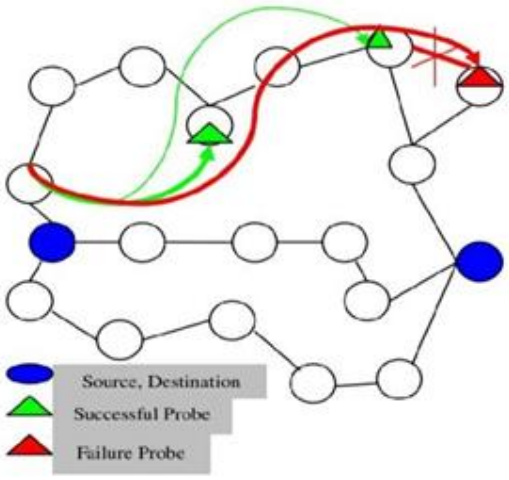


Figure 4. Binary Search Probing for Finding Faulty Links

The list of probes defines a set of non – overlapping intervals that covers the whole path where each interval covers the sub path between the consecutive probes that forms its end points as in Fig 4. When a fault is detected on an interval, the interval will be divided into two by inserting a new probe. This new probe is added to the list of probes appended to future packets. The process of subdivision continues until a fault is detected on the interval that corresponds to a single link. This result in finding log n faults where n is the length of the path.

D. Calculating the path metric

After a sender and a receiver start to exchange data packets, they build tables to keep traffic patterns. There is one table built by the sender and another one built by the receiver. The two tables have the same structure. Each table is composed of two fields: Packet identification number and time of action. Each time a packet is sent, the sender records the packet ID and the time. Each time a packet is received a receiver records the packet ID and the time. Every five (or t) seconds based on network environment, the receiver sends the sender a table. Upon receipt of the table from the receiver, the sender merges it with its own table into an anomaly detection table. The anomaly detection table contains packet identification, sending timestamp and receiving timestamp for each packet. Obviously, the sender gets the table refreshed every 5(or t) seconds. Using this information the sender can calculate the various values that will be mentioned in the following subsections and keep them in respective variables is received a receiver records the packet ID and the time.

1) Trip Time Variation: Trip time of each packet is the time a packet spends on the way, starting when it is transmitted, ending when it is received. That time is calculated using the sender's time stamp when a packet was sent and recipient's time stamps when a packet was received.
2) Change of packets frequency: The sender compares both the frequency at which packets were sent and the frequency at which packets were received, measured in packets per second. By comparing the two frequencies, delays of packets can be noticed.
3) Link Failures: Upon finding the link failure using binary search probes, all the paths containing that link will be discarded by decreasing the level of trust by half.
4) Trust Updation and Path Set Selection

An initial value is assigned to the variable of trust related to a path. A threshold is set based on expected behaviour of the network environment .Based on the observation the paths metrics are updated and are used as a parameter while selecting the active path set.

5) Emergency situation awareness<AN CASE STUDY>

A wireless network formed by the mobile devices can reduce lack of situation awareness in areas prone to emergencies, and support the management of emergency activities. The network nodes that are free to move and organize themselves can gather data from many sources and transmit them to the central dispatcher. In presented case study we focus on emergency situation at the airport The goal was to create the coherent IEEE 802.15.4 based wireless network for on-line monitoring of the arrival hall (90m×90m).

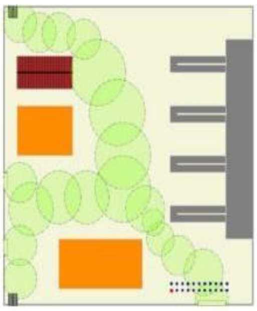


Fig. 14 The initial network topology

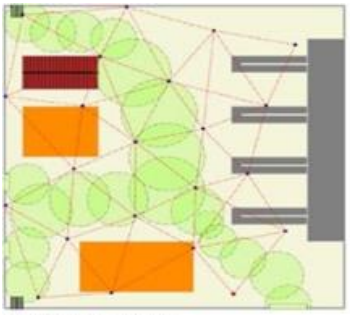


Fig. 15 The final network topology

The The initial network topology Mobile Netw Appl The final network topology plan of the arrival hall is presented. The network was composed of 22 mobile devices calculating their motion patterns due to the COHERENT NET algorithm. Fig. 14 presents the initial topology of the network. The results of the simulation of 200 seconds of network formation process are presented in Fig. 15 and in Table 1. From these results we can see that the final topology of the network is close to the expected one (most nodes reached their targets). However, the number of nodes assumed in this experiment was too small to create the optimal topology and satisfy all constraints.

IV.CONCLUSION

In this paper, we focused on mobility modeling in indoor and outdoor scenarios and proposed a novel approach to cooperative mobile network design. We mainly aimed to brief about the history application of MANET technologies basically in military applications rescue operations and many in a presice manner .Our approach combines techniques based on the potential field and the particle based scheme for the motion paths computation.

V. REFERENCES

[1]. Papadimitratos, P. Haas, Z.J , "Secure data communication in mobile adhoc networks" , This paper appears in: Selected Areas in Communications, IEEE Journal on Publication Date: Feb. 2006,Volume: 24, Issue: 2,On page(s): 343- 356.

[2]. Reza Curtmola Cristina Nita-Rotaru, " BSMR: Byzantine-Resilient Secure Multicast Routing in Multihop Wireless Networks" , IEEE Transactions on Mobile Computing, vol. 8,Issue. 4,pp. 445 - 459,February 2009.

[3]. A.Tsirigos and Z.J.Hass (2004) , "Analysis of mulitipath routing, Part 1: The effects on the packet delivery ratio" IEEETransactions on Wireless Communication., vol.3, no.2,pp:500-511

[4]. Banner, R. Orda, A , "Multipath Routing Algorithms for Congestion Minimization". This paper appears in: Networking,IEEE/ACM Transactions on Publication Date: April 2007 Volume: 15, Issue: 2,On page(s): 413-424.

[5]. P.Papadimitratos and Z.J.Hass, " Secure Routing For Mobile Ad-Hoc Networks", in proceeding of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS-2002).

[6]. Papadimitratos, P. Haas, Z.J and E.G.Sirer , " Path set selection in mobile ad hoc Networks" ,in Proc 3rd ACM MobiHoc , Lausanne, Switzerland, Jun 2002 ,pp 1-11.

[7]. C.Siva Ram Murthy and B.S Manoj.,(2004), "Ad Hoc Wireless Networks- Architecutres and Protocols" , Pearson Education.

[8]. Kołodziej J, Khan SU, Wang L, Min-Allah N, Madani SA, Ghani N, Li H (2011) An application of markov jump process model for activity-based indoor mobility prediction in wireless networks.In: 9th IEEE international conference on frontiers of information technology (FIT). Islamabad, pp 51–56 Mobile Netw Appl

[9]. Musolesi M, Mascolo C (2009) Mobility models for systems evaluation. A survey. State of the art on middleware for network eccentric and mobile applications (MINEMA).Springer

[10]. Mostafi Y (2011) Compressive sensing on mobile computing.IEEE Trans Mob Comput 10(10):1769– 1784

[11]. Niewiadomska-Szynkiewicz E, Sikora A (2011) Simulation-based design of self-organising and cooperative networks. Int J Space Based Situated Comput 1(1):68–75

[12]. A. Altay Yavuz, F. Alag¨oz , E. Anarım, A new satellite multicast security protocol based on elliptic curve signatures, IEEE International Conference on Information Communication Technologies (ICTTA) , April 2006, Syria.

[13]. A. Altay Yavuz, F. Alag¨oz, E. Anarım, Three-Tiers satellite multicast security protocol based on ECMQV and IMC methods, Computer-Aided Modeling, Analysis and Design of Communication Links and Networks (CAMAD'06),April 2006, Italy.

[14]. A. Altay Yavuz, F. Alag¨oz, E. Anarım, NAMEPS: N -Tier Satellite Multicast Security Protocol Based on Signcryption Schemes, IEEE Globecom Conference, San Francisco, November 2006.

[15]. W. Diffie, M. Hellman, New directions in cryptography, IEEE Transactions on Information Theory, Vol:.22, No.6, pp. 644–654, Nov. 1976.

Cite this article as :

Goutham S Tantri, Manjunatha M J, "Army Security Communication Network - An Review on Inter Tactical Mobile Ad Hoc Network Routing Protocol", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 01-08, September-October 2019. Journal URL : http://ijsrcseit.com/CSEIT19471