International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

A Study of Security Challenges and Solutions in Mobile Ad-Hoc Network

Thangaraj E[1], Dinesh Ruban J[2]

[1]St.Joseph University in Tanzania –Arusha Campus, Department of Computer Science, Arusha- 14425, Tanzania,

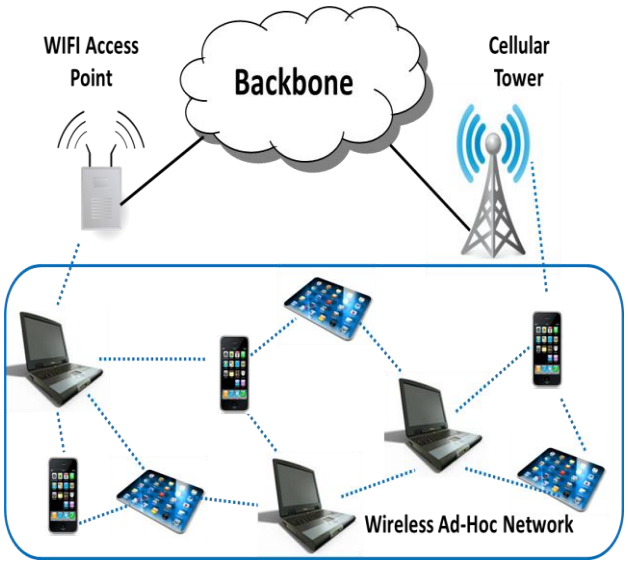
[2]St. Joseph College of Engineering and Technology in Tanzania, Department of Computer science & Engineering, Dar es Salaam 11007, Tanzania

Abstract: ***Mobile Ad Hoc Network (MANET) is a more number of communication devices or nodes that to communicate without any fixed infrastructure and pre-determined organization of current links. The nodes in MANET themselves are responsible for dynamically discovering other nodes to communicate. Even though the new trend is to adopt ad hoc networks for commercial uses due to their unique properties, the import challenge is the vulnerability to security attacks. A more number of challenges like open peer-to-peer network architecture, shared wireless medium, dynamic network topology etc. As MANET is quickly spreading for the property of its capability in making temporary network without the aid of any established infrastructure or distributed administration, security challenges has become a important concern to provide secure communication. In this paper we find the existent security threats an ad hoc network faces, the security services required to be achieved and the countermeasures for attacks in each layer. In our study, we have found that necessity of secure routing protocol is still have question. There is no general algorithm that suitable for well against the most commonly known attacks such as wormhole, rushing attack etc. In finally, we focus on the findings and future works which may be for the researchers like robust key management, trust based systems, data security in different layer. However, in short, we can say that the complete security solution requires the prevention, detection.***

Keywords: Hybrid routing protocols, Distance Vector Routing, Dynamic Source Routing, Ad Hoc On Demand Distance Vector, Message authentication code.

1. Introduction

A mobile ad-hoc network is a continuously own–configuring, infrastructure –less network of mobile devices connected without physical connection. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forwarded traffic unrelated to its own use, and therefore be a router. The important challenge in building MANET is equipping each device to continuously maintain the information required properly route traffic. Such networks may be activate by themselves or may be connected to the larger internet. They may contain one or more and different transceivers between nodes. MANET is kind of wireless ad-hoc network that usually has a routable networking environment on top of link layer ad-hoc network. MANETs consists of a peer-to-peer, self-forming, self-healing network. These attributes enable MANETs to deliver important benefits in virtually any scenario that includes a cadre of highly mobile users or platforms, a strong need to share IP-based information.



Mobile ad hoc network having different challenges with wireless security due to some of the following reasons:

1) The wireless network especially liable to attacks because of active eavesdropping to passive interfering.
2) Due to lack of Trusted Third Party adds, it is very difficult to deploy or implement security mechanisms.
3) Mostly Mobile devices have limited computation capability and power consumption functionalities which are more vulnerable to Denial of Service attacks. It is also incapable to run heavy security algorithms which need high computations like public key algorithms.
4) Due to MANET"s properties like infrastructure less and self-organizing, there are more chances for trusted node to be compromised and launch attacks on networks. In other words we need to cover up from both insider and outsider

attacks in MANET, in which insider attacks are more difficult to deal with.

5) It is very difficult to distinguish between stale routing and faked routing information because of node mobility mechanism. In node mobility mechanism it enforces frequent networking reconfiguration which creates more chances for attacks.

2. Problem Definition

One of the important characteristic of MANET‟s with to the security design point of view is the lack of clear line defense. In case of wired networks we have dedicated routers; which perform routing functionalities for devices but in case of Mobile ad hoc network are concerned each mobile node acts as a router and forward packets for other nodes. It is also true that the wireless channel is access to both network users as well as to attackers. There is no well-defined rule or place where traffic from one to another node should be monitored or access control mechanisms can be enforced. Due to this way there is no any defense line that alone inside network from the outside network. Due to this way the existing ad hoc routing protocols, like Dynamic Source Routing (DSR) and Ad Hoc On Demand Distance Vector (AODV) , and wireless MAC protocols.

3. Routing Protocol Description:

There are basically there kind of routing protocols which are:

3.1 Table Driven Routing Protocols

In these routing protocols every node in the network maintains the complete routing information of the network by occasionally updating the routing table, so when a node required to send some data or information, so there is no any kind of delay for discovering the route in the whole network. This type of routing protocols approximately works the same way as the wired network routing protocol works. The table driven protocols are DSDV and WRP.

3.2 On-Demand Routing Protocols

While in this kind of routing protocols, a node simply maintains routes information to get destination that it needs to send required data packets. The routes to get their desire destinations will expire automatically after some time of idleness, while the network is not being used. These routing protocols are AODV, DSR and TORA.

3.3 Hybrid Routing Protocols (ZRP)

In this type of routing protocol is the combined of the above two categories. In which nodes belonging to geographical area or within a certain detachment from an anxious node are said to be in routing area and uses table driven routing protocol. Communication between nodes in different areas will rely on the source initiated or on-demand routing protocols. This routing protocol is a ZRP.

3.4 AODV

AODV is a classical distance vector routing algorithm. It is also shares DSR‟s on-demand discovers routes. When repairing link breakages AODV use to provide loop free routes. It does not add any overhead to the packets, whenever a route is available from source to destination. Due to this way it reduces the effects of stale routes and also need for route maintenance for unused routes. One of the best advantages of AODV is to provide broadcast, unicast and multicast communication. During route discovery algorithm AODV uses a broadcast and for reply it uses unicast.

3.5 DSR

The DSR is an on-demand routing protocol that is based on source routing. It uses no periodic routing messages and due to this way it reduces network bandwidth overhead, and also remove the large routing updates as well as it also decrease conserves battery power. In order to find link layer failure DSR needs support from the MAC layer. It is contain the two network processes, Route Discovery and Route Maintenance. Both of neither AODV nor DSR guarantees shortest path.

3.6 TORA

The TORA is an adaptive, scalable and resourceful distributed routing algorithm. It is mainly designed for multi-hop wireless networks as well as extremely dynamic mobile atmosphere. It is also called source-initiated on-demand routing protocol. It is also use to find multiple routes from source to destination node. One of the main advantages is that the control messages are localized to a very small set of nodes near to seem of the topological change. It has three basic functions: Route maintenance, Route elimination and Route establishment.

4. Security

The goals of Mobile Ad hoc network have in contemporary years not only seen extensive use in commercial and internal application areas but have also become the focus of concentrated research. Uses of MANET‟s range from simple wireless home and office networking to sensor networks and similarly self-conscious tactical network atmospheres. Security features play an vital role in almost all of these application scenarios given the vulnerabilities inherent in wireless ad hoc networking from the very fact that radio communication takes place to routing, man-in-the-middle and elegant data injection attacks.

4.1 Protecting Mobile ad-hoc network.

An ad hoc routing protocol is a concord, or typical, that controls how nodes decide which way to route packets between computing devices in a mobile ad-hoc network. In ad hoc networks, nodes do not start out familiar with the topology of their networks; instead, they have to discover it. The basic idea is that a new node may announce its presence and should listen for announcements broadcast by its neighbors. Each node learns about nodes nearby and how to

reach them, and may announce that it, too, can reach them. Note that in a wider sense, ad-hoc protocol can also be used literally, that is, to mean an improvised and often impromptu protocol established for a specific purpose.

4.2 Reactive Approach

Seeks to detect security threats and react accordingly. This type of protocols maintains fresh lists of destinations and their routes by periodically distributing routing tables throughout the network. The main disadvantages of such algorithms are:
1) Respective amount of data for maintenance.
2) Slow reaction on restructuring and failures.

There are two main things in re-active routing protocols first is that it never take initiative in order to take routes for network, second is that whenever it creates routes it will developed on demand by flooding mechanism. In such kind of routing protocols there are some advantages and disadvantages which are given below:
Whenever they need to find out the routes they use bandwidth otherwise it will not use bandwidth. There is lot of overhead because of the flooding process. At start there is delay in the network.

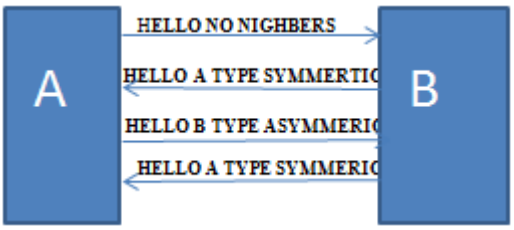
There are three steps which will explain the complete procedure of the re-active routing protocols.
1) If there are two nodes at position A and position B which want to communicate.
2) In order to communicate with the B, A needs to flood the routes towards the B.
3) In order to create communication between A and B unicast feedback will come back.

Efforts to avoid an attacker from launching attacks through various cryptographic techniques:

In pro-active routing protocols the method is different than the re-active routing protocols. In this type of protocols basically routes are depends upon the traffic control which is continuous. All routing information maintained at any time of the network because we know that network is self-motivated which changes its size by making its size increasing or decreasing.
There are three steps in pro-active routing algorithm which are given below:
1) Link/ Neighbor Sensing.
2) Multipoint Relaying.
3) Link-State messaging and route calculation.

4.3.1 Link / Neighbor Sensing

In Link and Neighbors sensing method we know by its name that neighbors and links are developed association among each other by transfer hello packets to each other so that there will be connectivity between the different devices. In mobile ad hoc network all nodes or devices send hello packets among each other due to this system association between the neighbors and links has been made.



4.3.2 Multipoint Relaying

In multipoint Relaying method whenever the devices send hello packets to every other or we can say that every node send broadcast hello packet to every other node except for itself due to this way a lot of duplicate packets will create in order to overcome these duplicate retransmission multipoint relaying mechanism is used which will shrink the duplicate packets in broadcast packets. It will also limits other nodes or devices that at some regular time of intermission you have to send the broadcast packets in order to know about the connectivity amongst the neighbors and links

4.3.3 Link-State messaging and route calculation

In multipoint relay selection mechanism every node in the network has to developed or maintain its own Multipoint Relaying procedure in order to run the protocol. One of the basic rule is that if there is a two nodes and they are neighbors to each other. In forwarding of traffic step all nodes from the network has to established or maintain each and every node their own Multipoint Relaying Selectors. There is one basic rule for forwarding traffic that is whenever we are going to follow the pro-active routing protocols then all the packets from the routing protocols has been received by the Multipoint Relaying selector then packet is forward whenever its TTL value is greater than 0 due to this way packets will reach its all required destination in the network.

4.3.4 Link State functionality

The key functionality of Link State is that all devices in the network will flood out or broadcast link State information among the devices or nodes in order to make nodes updated. Multipoint Relaying selectors are used for forwarding routes so that"s why its better to be used for forwarding link state information that"s why Multipoint Relaying selectors are selected to send link state messages due to this way size will decreases which is very useful in link state messages.

We know that before forwarding routes there is a selection for Multipoint Relaying procedure so those nodes or devices which are choose as a Multipoint Relaying then only those devices and nodes are responsible for ending link state messages.

5. Attacks

The modern Mobile ad hoc networks allow for a number of different types of attacks. Although the analogous exploits also exist in wired networks but it is easy to fix by infrastructure in such a network. Present MANETs are mainly vulnerable to two different types of attacks: active attacks and passive attacks. Active attack is an attack when misbehaving node has to allow some energy costs in order to perform the threat. On the other hand, passive attacks are

mainly due to lack of co-operation with the resolve of saving energy selfishly. Nodes that perform active attacks with the aim of damaging other nodes by affecting network outage are considered as malicious while nodes that create passive attacks with the purpose of saving battery life for their own communications are considered to be selfish. In this chapter, our focus is on vulnerabilities and exposures in the present ad hoc network. We have classified the attacks as modification, impersonation, fabrication,wormhole and lack of co-operation.

5.1 Attacks Using Modification

Modification is a type of attack when an unauthorized person not only achievements access to tampers with an asset. For example a malicious node will be redirect the network traffic and conduct Denial of services attacks by altering message fields or by forwarding routing message with incorrect values. In below diagram M is a malicious node which can preserve traffic from reaching S1 by continuously advertising to B a shorter route to S1 than the route to S1 that C advertises. In this method, malicious nodes can simply cause traffic subversion and denial of service by simply changing protocol fields: such attacks cooperation the integrity of routing computations. Through modification, an attacker can cause network traffic to be dropped, redirected to a different destination or to a longer route to reach to destination that causes unnecessary communication delay.

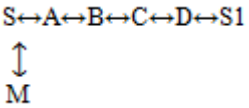


Figure 1: Ad hoc network and a malicious node

Consider the following fig 1 Assume a shortest path exists from S to S1 and, C and S1 cannot hear each other, that nodes B and C cannot hear other, and that M is a malicious node attempting a denial of service attack. Suppose S needs to communicate with S1 and that S has an unexpired route to S1 in its route cache. S transfers a data packet toward S1 with the source route S --> A --> B --> M --> C --> D --> S1 contained in the packet‟s header. When M receives the packet, it can alter the source route in the packet‟s header, such as deleting D from the source route. Consequently, when C receives the altered packet, it attempts to toward the packet to S1. Since S1 cannot hear C, the transmission is unsuccessful.

S↔A↔B↔M↔C↔D↔S1

Figure 2: Ad hoc network with Dos attack

5.2 Attacks Using Impersonation

As there is no authentication of data packets in current ad hoc network, a malicious node can launch many attacks in a network by masquerading as another node i.e. spoofing. Spoofing is occurred when a malicious node misrepresents its identity in the network (such as altering its MAC or IP address in outgoing packets) and alters the target of the network topology that a benign node can gather. As for example, a spoofing attack allows forming loops in routing packets which may also result in partitioning network. Here we have defined the scenario in details.

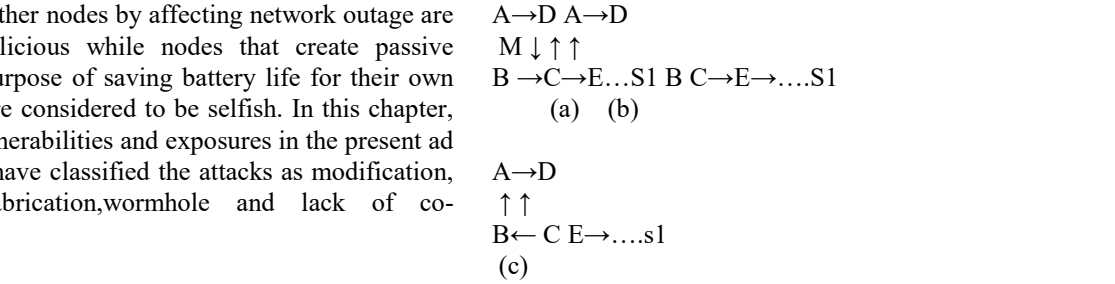


Figure: Sequence of events forming loops by spoofing packets

In the above fig. (a), there exists a path between five nodes. A can hear B and D, B can hear A and C, D can hear A and C, and C can hear B, D and E. M can hear A, B, C, and D while E can hear C and next node in the route towards S1. A malicious node M can learn about the topology analyzing the discovery packets and then form a routing loop so that no one nodes in his range can reach to the destination S1. At first, M changes its MAC address to match A‟s, moves closer to B and out of the range of A. It sends a message to B that contains a hop count to S1 which is less than the one sent by C, for example zero. Now B changes its route to the destination, S1 to go through A as shown in the fig.(b). Similarly, M again changes its MAC address to match B‟s, moves closer to C and out of the range of B. Then it sends message to C with the information that the route through B contains hop count to S1 which is less than E. Now, C changes its route to B which forms a loop as shown in fig. (c). Thus s1 is unreachable from the four nodes in the network.

5.3 Attacks through Fabrication

Fabrication is an attack in which an unauthorized party not only gains the access but also inserts counterfeit objects into the system. In MANET, fabrication is used to refer the attacks performed by generating false routing messages. Such kind of attacks can be difficult to verify as they come as valid constructs, especially in the case of fabricated error messages that claim a neighbor cannot be contacted . Consider the fig.1. Suppose node S has a route to node S1 via nodes A, B, C, and D. A malicious node M can launch a denial-of-service attack against S1 by continually sending route error messages to B spoofing node C, indicating a broken link between nodes C and S1. B receives the spoofed route error message thinking that it came from C. B deletes its routing table entry for S1 and forwards the route error message on to A, who then also deletes its routing table entry. If M listens and broadcasts spoofed route error messages whenever a route is established from S to S1, M can successfully prevent communications between S and S 1.

5.4 Wormhole Attacks

Wormhole attack is also known as tunneling attack. A tunneling attack is where two or more nodes may collaborate to encapsulate and exchange messages between them along existing data routes. This exploit gives the opportunity to a node or nodes to short-circuit the normal flow of messages

creating a virtual vertex cut in the network that is controlled by the two colluding attackers.

5.5 Lack of Cooperation

Mobile Ad Hoc Networks (MANETs) rely on the cooperation of all the participating nodes. The more nodes cooperate to transfer traffic, the more powerful a MANET gets. But one of the different kinds of misbehavior a node may exhibit is selfishness. A Selfishness node wants to preserve own resources while using the services of others and Consuming their resources. This can endanger the correct network operation by simply Not participating to the operation or by not executing the packet forwarding.

6. Countermeasures

6.1 Countermeasures on Physical Layer Attacks:

The physical layer of MANET is immune to signal jamming, Denial of Service attack and also some passive attacks. Two spread spectrum technologies can be used to make it difficult to detect or jam signals. Spread spectrum technology changes frequency in a random fashion or spreads it to a wider spectrum which makes the capture of signal difficult. The FHSS (Frequency Hopping Spread Spectrum) makes the signal indecipherable duration impulse noise to the eavesdroppers. On the other hand, DSSS (Direct Sequence Spread Spectrum) represents each data bit in the original signal by multiple bits in the transmitted signal through 11-bit Barker code. However, both FHSS and DSSS pose difficulties for the malicious user while trying to intercept the radio signals. To capture and release the content of transmitted signal, the attacker must know frequency band, spreading code and modulation techniques. Still, there is a problem. These mechanisms are secure only when the hopping pattern or spreading code is unknown to the eavesdropper.

6.2 Countermeasures on data Link Layer Attacks:

The security issues that are closely related to link layer are protecting the wireless MAC protocol and providing link-layer security support. But recently a security extension to 802.11. The original 802.11 back off scheme is slightly modified in that the back off timer at the sender is provided by the receiver instead of setting an arbitrary timer value on its own. As mentioned earlier, the threats of resource consumption (using NAV field) is still an open challenge though some schemes have been proposed such as ERA-802.11. Finally, the common known security fault in link layer is the weakness of WEP. Fortunately, the 802.11i/WPA has restored all obvious loopholes in WEP and future countermeasures such as RSN/AESCCMP are also being developed to improve the strength of wireless security.

6.3. Countermeasures on Network Layer Attacks

Network layer is more vulnerable to attacks than all other layers in MANET. A variety of security threats is imposed in this layer. Use of secure routing protocols provides the first line of defense. The active attack like modification of routing messages can be prevented through source authentication and message integrity mechanism. For example, digital signature, message authentication code (MAC), hashed MAC (HMAC), one-way HMAC key chain is used for this purpose. By an unalterable and independent physical metric such as time delay or geographical location can be used to detect wormhole attack. For example, packet leashes are used to combat this attack. IPsec is most commonly used on the network layer in internet that could be used in MANET to provide certain level of confidentiality. The secure routing protocol named ARAN protects from various attacks like modification of sequence number, modification of hop counts, modification of source routes, spoofing, fabrication of source route etc, al presents a solution to overcome black hole attack. The solution is to disable the ability to reply in a message of an intermediate node, so all reply messages should be sent out only by the destination node.

6.4. Countermeasures on Transport Layer Attacks.

One way to provide message confidentiality in transport layer is point-to-point or end-to end communication through data encryption. Though TCP is the main connection oriented reliable protocol in Internet, it does not fit well in MANET. TCP feedback (TCP-F) TCP explicit failure notification (TCP-ELFN), Ad-hoc transmission control protocol (ATCP) and ad hoc transport protocol (ATP) has been developed but none of them covers security issues involved in MANET. Secure Socket Layer (SSL) ,Transport Layer Security (TLS) [9] and Private Communications Transport (PCT) protocols were designed on the basis of public key cryptography to provide secure communications. TLS/SSL provides protection against masquerade attacks, man-in middle attacks, rollback attacks, and replay attacks.

6.5. Countermeasures on Application Layer Attacks

Viruses, worms, spywares, Trojan horses are the common and challenging application layer attacks in some network. Firewall provides defense gains particular of these attacks. For example, it can deliver access control, user authentication, incoming and outgoing packet filtering, network filtering, accounting service etc. Anti-spyware software can detect spyware and malicious programs running on the system. Still using firewall is not enough for the reason that in certain situation the attacker even can penetrate firewall and make an attack. Another method, Intrusion Detection System (IDS) is effective to avoid certain attacks such as trying to gain unauthorized access to a service, pretending like a legitimate user etc. The application layer also detects a Denial of service attack more quickly than the lower layers.

7. Conclusion

Mobile Ad Hoc Networks have the capacity to setup networks on the fly in strict platforms where it could not promising to deploy a outdated network infrastructure. Whether ad hoc networks have huge potential, still there are many challenges left to overcome. Security is a vital feature

for deployment of MANET. In this paper, we have overviewed the encounters and solutions of the security threats in mobile ad hoc Networks. The first research question is „whatever are the vulnerabilities and security threats in MANET? Which level is most vulnerable to attack?" In our study, we present a so many attacks associated to different layers and discovery that network layer is most vulnerable than all other layers in MANET. This separation of attacks on the root of different layers makes easy to understand about the security attacks in ad hoc networks. „How the security services like confidentiality, integrity and authentication can be achieved from mobile ad hoc networks? What ladders should be taken?" is the second research question. The answer is that security services can be achieved through following the preemptive and responsive countermeasures on the root of particular attack. In addition, we can say that security must be confirmed for the entire system since a single weak point may provide the attacker the opportunity to increase the access of the system and perform malicious tasks. The final research question is „what are the potential hazards that may be vital in future?" Every day, the attackers are trying to find out the new vulnerability in MANET.

8. Future Enhancements

Important research in MANET has been ongoing for many years, but still in an early stage. Present solutions are well-matched only for particular attack. They can scope well with Known attacks but there are several unanticipated or joined attacks left over unexposed. Resource used Denial of Service attack is still unresolved. More needed on secure routing protocol, robust key management, and trust based systems, integrated approaches to routing security, data security in different level and co-operation enforcement. Present routing protocols are subject to a several attacks that can allow attackers to influence a victim"s selection of routes or enable denial-of service attack. So, need of secure routing protocol is inevitable. Cryptography is one of the most common ecurity methods and its strength relies on the secure key management. The public cryptography system depends upon centralized CA (Certificate Authority) which is known as a security weak point in MANET. Symmetric cryptography is efficient but hurts from possible attack on key distribution. Hence, effective key agreement and distribution in MANET is an ongoing research area.

9. Acknowledgement

I would like to thank my family and Sr.Ramona for their valuable encouragement and special thanks to Mr.P.Arumuga samy and the staff members from the St. Joseph University for their Technical Support to us.

References

[1] Kamanshis Biswas and Md. Liakat Ali "Security Threats in Mobile Ad Hoc Network" Master Thesis Computer Science Thesis no: MCS-2007:07 22nd March, 2007.
[2] Nikhil Varghane, Prof. Bhakti Kurade, Prof. Chandradas Pote "Intrusion Detection, Secure Protocol & Network Creation for Spontaneous Wireless AD HOC Network" IJCSMC, Vol. 3, Issue. 2, February 2014.
[3] Amandeep Verma and Manpreet Singh Gujral "Trust Oriented Secure Ad hoc Networks: A Generic Framework" IJETCAS 13-399; © 2013.
[4] Muhammad Arshad Ali and Yasir Sarwar "Security Issues regarding MANET (Mobile Ad Hoc Networks): Challenges and Solutions" School Master Thesis Computer Science Thesis no: MCS-2011-11 March 2011.
[5] H Yang H Y. Luo F Ye S W. Lu L Zhang "Security in mobile ad hoc networks: Challenges and solutions" Year 2004.
[6] Lennart Isaksson "Improved Performance of Bluetooth with Focus on Ad-Hoc Applications" Published 2004 Printed by Kaserntryckeriet AB Karlskrona 2004 Sweden.
[7] Luis Javier García Villalba , Julián García Matesanz , Ana Lucila Sandoval Orozco and José Duván Márquez Díaz "Auto-Configuration Protocols in Mobile Ad Hoc Networks "Sensors 2011.

Author Profile

Mr. Thangaraj E. received the M. Tech in Computer Science and Engineering at Dr. M.G.R Educational and Research Institute University in Chennai and B. E degree in Computer Science and Engineering at Madurai Kamaraj University in Madurai. Presently he is working as a lecturer in ST. Joseph College of Engineering and Technology in Tanzania for the past 6 years. His area of interest is networking and cloud computing.

Mr. Dinesh Ruban. Received the M.E in VLSI Technology at SKR Engineering College, Poonamalle and B.Tech in information Technology at Infant Jesus College of Engineering, Tuticorin. Presently he is working as a lecturer in ST. Joseph College of Engineering and Technology in Tanzania for the past 2 years. His area of interest is networking and cloud computing.