ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

Energy Efficient Coverage Problems in Wireless Ad Hoc Sensor Networks

N. Vijayarani[1], C.Ramya[2]

Assistant Professor, Department of Computer Science, Selvamm Arts and Science College (Autonomous), Namakkal, India[1]

M. Phil Scholar, Department of Computer Science, Selvamm Arts and Science College (Autonomous), Namakkal, India[2]

ABSTRACT: Mobile Ad-hoc Networks (MANET) is a network consisting of a collection of nodes which can communicate with each other without help from a network infrastructure. There has been a growing interest in Mobile Ad hoc Networks (MANETs) motivated by the advances in wireless technology and the range of potential applications that might be realized with such technology. Due to the lack of an infrastructure and their dynamic nature, MANETs demand a new set of networking protocols to harness the full benefits of the versatile communication systems. The Cipher Block Chaining (CBC-X) mode is used to complete message authentication, encryption and decryption concurrently before sending message.

In order to provide the data integrity, an enhanced distributed certificate authority scheme (EDCA) is developed. This scheme makes the network more secure from both inside and outside attacks. It utilizes three components namely monitoring Routing Cum Forwarding (RCF), certificate revival and certificate revocation.RCF involves detectingmisbehaviors in both the routing as well as
the packet forwarding in the network. Certificate revocation provides the authority to isolate the malicious nodes or regain the nodes which turn up to its best state after any attack or failure. Certificate revival scheme is used for increasing the data integrity of the packets. In this revival scheme, every legitimate node carries a certificate which is issued by certificate authority to make the communication between the nodes inside the network. For providing certificate authority, the Shamir's secret sharing scheme and modified Shamir secret scheme are used.
It provides security as well as is extendable and flexible. Based on the results, it is observed that the enhanced distributed certificate authority scheme achieves more packet delivery ratio while attaining less delay and overhead than the trust based cross layer security protocol.

KEYWORDS: "Authority Scheme for Authentication in Mobile Adhoc Networks"

I. INTRODUCTION

Wireless cellular systems have been in use since 1980s.Wireless systems operate with the aid of a centralized supporting structure such as an access point. These access points assist the wireless users to keep connected with the wireless system, when users roam from one place to the other. The presence of a fixed structure limits the adaptability of wireless systems. In other words, the technology cannot work effectively in places where there is no fixed infrastructure. Future generation wireless systems will require easy and quick deployment of wireless networks. This quick network deployment is not possible with the existing structure of current wireless systems.

Recent advancements such as Bluetooth introduced a new type of wireless systems known as Mobile Ad-hoc Networks. Mobile Ad-hoc networks or "short live" networks operate in the absence of fixed infrastructure. It offers quick and easy network deployment in situations where it is not possible otherwise. Mobile ad-hoc network is an autonomous system of mobile nodes connected by wireless links. Each node operates as an end system and a router for all other nodes in the network. Nodes in mobile ad-hoc network are free to move and organize themselves in an arbitrary fashion. Each user is free to roam about while communication with others. The path between each pair of the

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

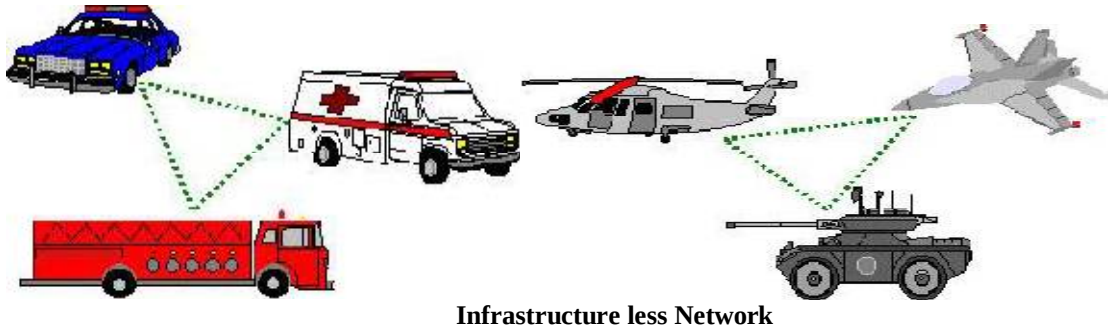
users may have multiple links and the radio between them can be heterogeneous. This allows an association of various links to be a part of the same network.

A mobile ad-hoc network is a collection of mobile nodes forming an ad-hoc network without the assistance of any centralized structures. These networks introduced a new art of network establishment and can be well suited for an environment where either the infrastructure is lost or where deploy an infrastructure is not very cost effective. Mobile ad-hoc networks can turn the dream of getting connected "anywhere and at any time" into reality. Typical application examples include a disaster recovery or a military operation. Not bound to specific situations, these networks may equally show better performance in other places.

II. OVERVIEW OF MANET

MANET is a self-configuring system of mobile routers linked by wireless links which consequently combine to form an arbitrary topology. Thus, the network's wireless topology may alter rapidly and unpredictably. However, due to the lack of any fixed infrastructure, it becomes complicated to exploit the present routing techniques for network services, and this provides some huge challenges in providing the security of the communication, which is not done effortlessly as the number of demands of network security conflict with the demands of mobile networks, largely due to the nature of the mobile devices.e.g. low power consumption, low processing load.

MANETs does not depend on pre-existing infrastructure or base stations. Network nodes in MANETs are free to move randomly. Therefore, the network topology of a MANET may change rapidly and unpredictably. All network activities, such as discovering the topology and delivering data packets, have to be executed by the nodes themselves, either individually or collectively. Depending on its application, the structure of a MANET may vary from a small, static network that is highly power-constrained to a large-scale, mobile, highly dynamic network. It is a group of autonomous mobile nodes or devices connected through wireless links without the support of a communications infrastructure. The topology of the network changes dynamically as nodes move and the nodes reorganize themselves to enable communications with nodes beyond their immediate wireless communications range by relaying messages for one another, i.e. multi hop.



Infrastructure less Network

MANET relies on the cooperation of all the participating nodes. The more nodes cooperate to transfer traffic, the more powerful a MANET becomes. But supporting a MANET is a cost intensive activity for a mobile node. Detecting routes and forwarding packets consumes network bandwidth, local CPU time, memory and energy. Therefore there is a strong motivation for a node to deny packet forwarding to others, while at the same time using their services to deliver own data. MANET has various potential applications, which are usually set up in situations of emergency for temporary operations or simply if there are no resources to set up elaborate networks. Some typical examples include emergency search-rescue operations, meeting events, conferences and battlefield communication between moving vehicles and soldiers. With the abilities to meet the new demand of mobile computation, the MANET has a very bright future.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

TYPES OF MANET

- Vehicular ad hoc networks (VANETs) are used for communication between vehicles and roadside equipment. Intelligent vehicular ad hoc networks (InVANETs) are a kind of artificial intelligence that helps vehicles to behave in intelligent manners during vehicle-to-vehicle collisions, accidents.
- Smart phone ad hoc networks (SPANs) leverage the existing hardware (primarily Bluetooth and Wi-Fi) in commercially available smart phones to create peer-to-peer networks without relying on cellular carrier networks, wireless access points, or traditional network infrastructure. SPANs differ from traditional hub and spoke networks, such as Wi-Fi Direct, in that they support multi-hop relays and there is no notion of a group leader so peers can join and leave at will without destroying the network.
- Internet based mobile ad hoc networks (iMANETs) are ad hoc networks that link mobile nodes and fixed Internet-gateway nodes. For example, multiple sub-MANETs may be connected in a classic Hub-Spoke VPN to create a geographically distributed MANET. In such type of networks normal ad hoc routing algorithms don't apply directly. One implementation of this is Persistent System's CloudRelay.
- Military or tactical MANETs are used by military units with emphasis on security, range, and integration with existing systems. Common waveforms include the US Army'sSRW.

III. PROPERTIES OF AD HOC ROUTING PROTOCOLS

Distributed operation The protocol should of course be distributed. It should not be dependent on a centralized controlling node. This is the case even for stationary networks. The difference is that nodes in an ad-hoc network can enter/leave the network very easily and because of mobility the network can be partitioned.
Loop free To improve the overall performance, the routing protocol to guarantee that the routes supplied are loop-free. This avoids any waste of bandwidth or CPU consumption.
Demand based operation To minimize the control overhead in the network and thus not wasting network resources more than necessary, the protocol should be reactive. This means that the protocol should only react when needed and that the protocol should not periodically broadcast control information.
Unidirectional link support The radio environment can cause the formation of unidirectional links. Utilization of these links and not only the bi-directional links improves the routing protocol performance.
Security The radio environment is especially vulnerable to impersonation attacks, so to ensure the wanted behavior from the routing protocol, some sort of preventive security measures are needed. Authentication and encryption is probably the way to go and the problem here lies within distributing keys among the nodes in the ad-hoc network.
Power conservation The nodes in an ad-hoc network can be laptops and thin clients, such as PDAs that are very limited in battery power and therefore uses some sort of stand-by mode to save power. It is therefore important that the routing protocol has support for these sleep-modes.
Multiple routes To reduce the number of reactions to topological changes and congestion multiple routes could be used. If one route has become invalid, it is possible that another stored route could still be valid. The routing protocol is saved from initiating another route discovery procedure.
Quality of service support Some sort of Quality of Service support is probably necessary to incorporate into the routing protocol. This has a lot to do with what these networks will be used for. It could for instance be real-time traffic support. None of the proposed protocols from MANET have all these properties, but it is necessary to remember that the protocols are still under development and are probably extended with more functionality.

IV. CLASSIFICATION OF ROUTING PROTOCOLS IN MANETS

Classification of routing protocols in MANET's can be done in many ways, but most of these are done depending on routing strategy and network structure. According to the routing strategy the routing protocols can be categorized as Table-driven and source initiated, while depending on the network structure these are classified as flat routing, hierarchical routing and geographic position assisted routing.

An ad hoc routing protocol is a convention .or standard, that controls how nodes decide which way to route packets between computing devices in a network. Various routing protocols available for Ad hoc networks are AODV,CGSR,DSDV,DSR,OLSR,WRP,ZRP etc.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

Table-Driven routing protocols(Proactive)

These protocols are also called as proactive protocols since they maintain the routing information even before it is needed . Each and every node in the network maintains routing information to every other node in the network. Routes information is generally kept in the routing tables and is periodically updated as the network topology changes. Many of these routing protocols come from the link-state routing . There exist some differences between the protocols that come under this category depending on the routing information being updated in each routing table. Furthermore, these routing protocols maintain different number of tables. The proactive protocols are not suitable for larger networks, as they need to maintain node entries for each and every node in the routing table of every node. This causes more overhead in the routing table leading to consumption of more bandwidth.

On Demand routing protocols(Reactive)

These protocols are also called reactive protocols since they don't maintain routing information or routing activity at the network nodes if there is no communication. If a node wants to send a packet to another node then this protocol searches for the route in an on-demand manner and establishes the connection in order to transmit and receive the packet .The route discovery usually occurs by flooding the route request packets throughout the network.

AD HOC ON-DEMAND DISTANCE VECTOR (AODV)

An Ad Hoc On-Demand Distance Vector (AODV) is a routing protocol designed for wireless and mobile ad hoc networks. This protocol establishes routes to destinations on demand and supports both unicast and multicast routing. AODV is a reactive protocol.

Ad-Hoc On-Demand Distance Vector (AODV) Routing Protocol:

Ad hoc On-Demand Distance Vector (AODV) created path to destination when required and is also known as reactive routing protocol. Only after certain nodes send route discovery message the routes are built so that it communicates or transmits data with each other. The source node, the destination node, and the intermediate nodes along the active route which deals with data transmission alone store the routing information. Memory overhead is decreased; use of network resources is minimized, and run well in high mobility situation. Three main procedures are involved in the AODV communication, path discovery, establishment and maintenance of the routing paths. AODV uses 3 types of control messages to run the algorithm, i.e. Request (RREQ), Route Reply (RREP) and Route Error (RERR) messages. The format of RREQ and RREP packet are shown in the following table.

RREQ field

Source Address	Request ID	Source Sequence No.	Destination Address	Destination Sequence No.	Hop Count

RREP field

Source Address	Destination Address	Destination Sequence No.	Hop Count	Life time

The route discovery procedure is issued when the source node wants to establish the communication with the destination node. All the accessible neighbors of the intermediate node receive the RREQ request. The intermediate node checks the request RREQ and if it's the destination node, the request from the source will be forwarded to other neighbor nodes. Each node stores the broadcast identifier before forwarding the packet and previous node number from which the request came. When there is no reply timer is used by the intermediate nodes to delete the entry. Intermediate nodes will keep the broadcast identifier and the previous nodes from which the reply came from are kept when reply is received. In order to detect whether the node has received the route request message previously or not, the broadcast identifier and the source ID are used. . It prevents redundant request receive in same nodes. The source node selects the

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

message based on the hop counts when more than one reply is received. The routing table is invalidated if the link breaks down due to node mobility. When the link is lost, all the destination will become unreachable and route error message is created which lists all of these lost destinations. The node sends the RERR upstream towards the source node. Route discovery is reinitiated once the source receives the RERR, if it still required the route.

V. DESTINATION SEQUENCED DISTANCE VECTOR (DSDV)

The conventional Bellman-Ford routing algorithm has been modified and a proactive routing protocol has been established known as destination sequenced distance vector (DSDV) routing protocol. At each of the node, a new attribute, sequence number is added by the protocol. The node transmits the packets to other nodes in the network, with the help of the routing table maintained at each node. This protocol is mainly used for the data exchange along changing and arbitrary paths of interconnection. The interconnections are not close to any base station.

Protocol Overview and Activities

In order to transmit packets and for connectivity to different stations in the network, routing table is maintained in each node in the network. The available destinations and the number of hops required to reach the destination in the routing table are listed in this table. The destination station provides a sequence number which is used for tagging the routing entry. The station transmits and updated its routing table at regular intervals in order to maintain the consistency. With the information of broadcasted packets, the accessible stations and the number of hops required to reach the particular station can be determined. The packets may be transmitted containing the layer2 or layer 3 addresses. When the nodes move within the network, the packets are transmitted periodically and the routing information is advertised by broadcasting or multicasting the packets. The routing table of the each mobile station has to be advertised by the DSDV protocol. Frequent update of the advertisement is essential, since the entries in the table changes very quickly. There should exist a possibility that the nodes should be able to locate its neighbors in the network by assigning shortest number of hops for a route to a destination. The new sequence number and the following information are maintained by the data broadcasted in each node.

- The destination address
- The number of hops required to reach the destination and
- The new sequence number, originally stamped by the destination

The hardware addresses, network address of the mobile host are also transmitted along with the routing tables. The transmitter created the sequence number and they are stored in the routing tables. Thus the forwarding decisions are made based on the new destination sequence number. All the hosts are updated with the new sequence number in order to decide on how to maintain the routing entry for that originating mobile host. Metric is incremented after receiving the route information and it transmits the information by

Advantages of DSDV

- DSDV protocol guarantees loop free paths.
- Count to infinity problem is reduced in DSDV.
- To avoid extra traffic with incremental updates instead of full dump updates.
- Path Selection: DSDV maintains only the best path instead of maintaining multiple paths to every destination. With this, the amount of space in routing table is reduced.

Limitations of DSDV

- Wastage of bandwidth due to unnecessary advertising of routing information even if there is no change in the network topology.
- DSDV doesn't support Multi path Routing.
- It is difficult to determine a time delay for the advertisement of routes.
- It is difficult to maintain the routing table's advertisement for larger network. Each and every host in the network should maintain a routing table for advertising. But for larger network this would lead to overhead, which consumes more bandwidth

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

APPLICATIONS OF MANETS

As MANETs do not require a fixed infrastructure they have a number of benefits and versatility for certain environments and applications:

- Military Use – providing communication when a network is not available or not considered to be secure or safe to use an existing infrastructure.
- Search and Rescue – providing a communication network when existing network is not available or destroyed.
- Sensor networks – allowing a large number of sensors to communicate that may not be in the easiest of locations to place on a traditional network.

OBJECTIVE OF THESIS

The overall objective of this work is to developthe trust based security scheme based on Cross layer as well as MAC layer approach and enhanced distributed certificate authority protocol. This objective intrinsically comprises several tasks that should be done to attain the final goal.

- To achieve the confidentiality and authentication of packets in routing layers in MANETs.
- To find the malicious node effectively using routing layer information.
- To provide the data integrity using certification schemes.
- To improve the packet delivery ratio and reduce the overhead, delay using trust based security scheme.

VI. LITERATURE SURVEY

The literature survey mainly focuses on the existing challenges, threats and the earlier methodologies followed to overcome certain problems.

General

Farooq Anjum has proposed an initial approach in which NID (Network Intrusion Detection) deals with information passing on the entire network between any pair of communicating hosts. while it is very good at detecting unauthorized outsider access, bandwidth theft, DOS, it is incapable of operating in encrypted networks and in high-speed networks. In addition, NID is effective when the network has certain chokepoints at which detection can be done. As is obvious the NID approach is not effective in ad-hoc networks on account of absence of any choke points in such networks. As a result one might have to depend on having the intrusion detection mechanisms on all or some of the hosts in the system.

Anand Patwardhan proposed a Collaborative Intrusion Detection Systems (IDS) is performing best in a densely populated MANET with limited mobility, and performing worse in a sparsely populated MANET with significant mobility. The effectiveness of collaborative IDS also depends on the amount of data that can be collected by each node. The longer the nodes are members of the MANET, the greater the availability of meaningful data for further analysis. The degree of mobility of each node in the network has a significant impact on its effectiveness. In a MANET with a high degree of mobility, if the number of routing error messages causes by legitimate reasons far exceeds the number of routing error messages caused due to the presence of malicious nodes, the effectiveness or benefit of such an IDS may be minimal.

Threats of MANET

The broadcasting nature of transmission and the nodes self routing environment opens up the perception of security in MANET. The security issue of MANET is of large concern taking into account its various factors like its open network, mobility factor and other factors. When taking into security aspects, the attacks on MANET can be classified into two; internal attacks and external attacks [2, 5, 10, 18]. Internal attacks are those attacks which are caused by inside node of a network. These attacks are produced by either malicious nodes or by selfish nodes inside a network. These internal attacks are tough to detect as nodes affected by such an attack generate themselves the valid signatures using their private keys. Examples of internal attack are internal eavesdropping, where the nodes extracts copy of all information and exploited it without the knowledge of other nodes and packet dropping. In external attacks, the attackers are from outside the network but cause damage or compromises network within the network. Attacks from

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

external nodes can be prevented from cryptographic techniques such as encryption and authentication. As per routing, external attacks can be divided into active and passive attacks. Active external attacks use to degrade or stops message flow between the nodes. Denial of Service (DoS) attacks, packet dropping or flooding of packets are some examples of active external attacks. Passive external attacks are formally done by compromising the nodes and extracting vital information of the network. In passive attack, the attacker does not disrupt the network operation but only extracts information to damage further network operation. These type of attacks are basically impossible to detect, thus making it hard to produce security for such attacks.

SECURITY ISSUES IN MANET

The MANETS set new challenges for network security and the need of an hour is to pay more attention to the security threats posed on the network. Following are the concerned issues in security of ad hoc networks:

Nodes Acting as Routers As nodes themselves are participating in relaying of messages, any malicious node in the network can easily misuse the message traffic either by dropping messages or by generating false messages etc.

Limited Resources Due to the limitation of network resources in mobile ad hoc networks, the various cryptographic solutions applicable to wired networks are not directly applicable. Therefore there is a need for new security solutions which can find their application in this challenging domain.

Mobility of Nodes Dynamically changing network topology results in more opportunities for the malicious nodes to attack.

Location of Nodes Since Ad hoc networks are formed for a purpose, the deployment environment may not be very security sensitive. For Example, the nodes deployed in the battlefield or in the forests for tracking wild animals etc. may invite many security threats and attacks. 5. Wireless Medium: Interoperability is very easy in a wireless medium. Therefore, there is a lack of privacy and the important messages can be eavesdropped and modified easily.

VII. EXISTING SYSTEM

Security Threats in MANETS

An adhoc network can be attacked from any direction at any node which is different from the fixed hardwired networks with physical protection at firewall and gateways. Altogether it denotes that every node should be equipped to meet an attacker directly or indirectly. Malicious attack can be initiated from both inside and outside of the network. Tracking a specific node is difficult in large adhoc networks and hence, it is more dangerous and much difficult to detect the attacks from an affected node. Altogether it denotes that every node should be prepared to work in a way that it should not trust on any node immediately.

Distributed architecture should be applied in order to achieve high availability. This is because if the central entity is used in the security solution, it causes serious attack on the entire network when the centralized entity gets affected. The following are the types of active attacks and its relevant solutions: **Black hole attack**

Let H be a malicious node. When H receives a Route Request, it sends back a Route Reply immediately, which constructs the data and can be transmitted by itself with the shortest path. So S receives Route Reply and it is replaced by H -> S. Then H receives all the data from S.

Neighbor attack The neighbor attack and the black hole attack prevent the data from being delivered to the destination. But the neighbor attacker does not catch and capture the data packets from the source node. It leaves the settings as soon as sending the false messages.

Wormhole attack Two malicious nodes share a private communication link between them. One node captures the traffic information of the network and sends them directly to other node. Warm hole can eavesdrop the traffic, maliciously drop the packets, and perform man-in- the-middle attacks against the network protocols.

DoS (Denial of Service) attack When the network bandwidth is hacked by a malicious node , then it results to the DoS attack. In order to utilize precious network resources like bandwidth, or to utilize node resources like memory or computation power, the attacker inserts packets into the network. The specific instances of the DoS attack are the routing table overflow attack and energy consumption attack.

Information Disclosure attack The information disclosure attack aims at the privacy requirements of network. The confidential information's likerouting location, node status or secret keys and password are leaked out by the malicious node to the unauthorized nodes.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

Rushing attack The rushing attack aims against on-demand routing protocols which uses identical suppression at each node. In order to find routed to the destinations, the source nodes sends out the RREQ. Each intermediate node processes only the first non-duplicate packet and discards any duplicate packet which arrives at a later time. Rushing attackers can forward these packets quickly by skipping some of the routing processes. They are also able gain access to the forwarding group .

Jellyfish attackA malicious node receives and sends RREQ and RREP normally. But before forwarding it delays the data packets without any reason for some time. Since the node has to intrude the forwarding group first, it is difficult to implement this type of attack. If the number of malicious node is few, then the influence to the network is also less.

Byzantine attack(Impersonation attack) It is also called as impersonation attack because the malicious node might imitate another normal node. It also sends false routing information for creating an anomaly update in the routing table. In addition to this, an attacker may get unauthorized admission to resource and sensitive information.

Blackmail attack This attack is applicable against routing protocols which uses mechanisms for the recognition of malicious nodes and broadcast the messages which try to blacklist the offender . By adding other legitimate nodes to their blacklists, an attacker might blackmail a legitimate node. Thus the nodes can be avoided in those routes.

Overview of the Protocol

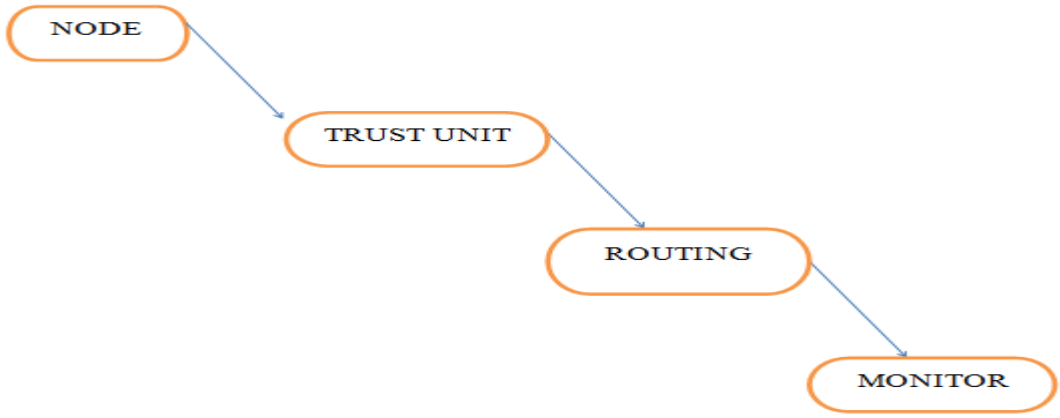
A Trust based packet forwarding scheme in MANETs without using any centralized infrastructure. It uses trust values to favor packet forwarding by maintaining a trust counter for each node. A node is punished or rewarded by decreasing or increasing the trust counter. Each intermediate node marks the packets by adding its hash value and forwards the packet towards the destination node. The destination node verifies the hash value and check the trust counter value. If the hash value is verified, the trust counter is incremented, other wise it is decremented. If the trust counter value falls below a trust threshold, the corresponding the intermediate node is marked as malicious. This scheme presents a solution to node selfishness without requiring any pre-deployed infrastructure. It is independent of any underlying routing protocol.

The CBC-X mode Encryption/Decryption algorithm to satisfy the necessity of minimum computational and communication overhead. This algorithm supports encryption/decryption and authentication of packets on a onepass operation. The upper layers of the protocol stack are provided with security services obviously. A CBC-X mode symmetric key mechanism is devised to employ our link layer security system. Encryption/Decryption and authentication operations are included into a single step which reduces the computational overhead to half, instead of calculating them individually. The padding technique states that this method has no cipher text expansion for the transmitted data payload. Thus the communication overhead is reduced significantly.

VIII. DATA FLOW DIAGRAM

LEVEL 0

LEVEL 1



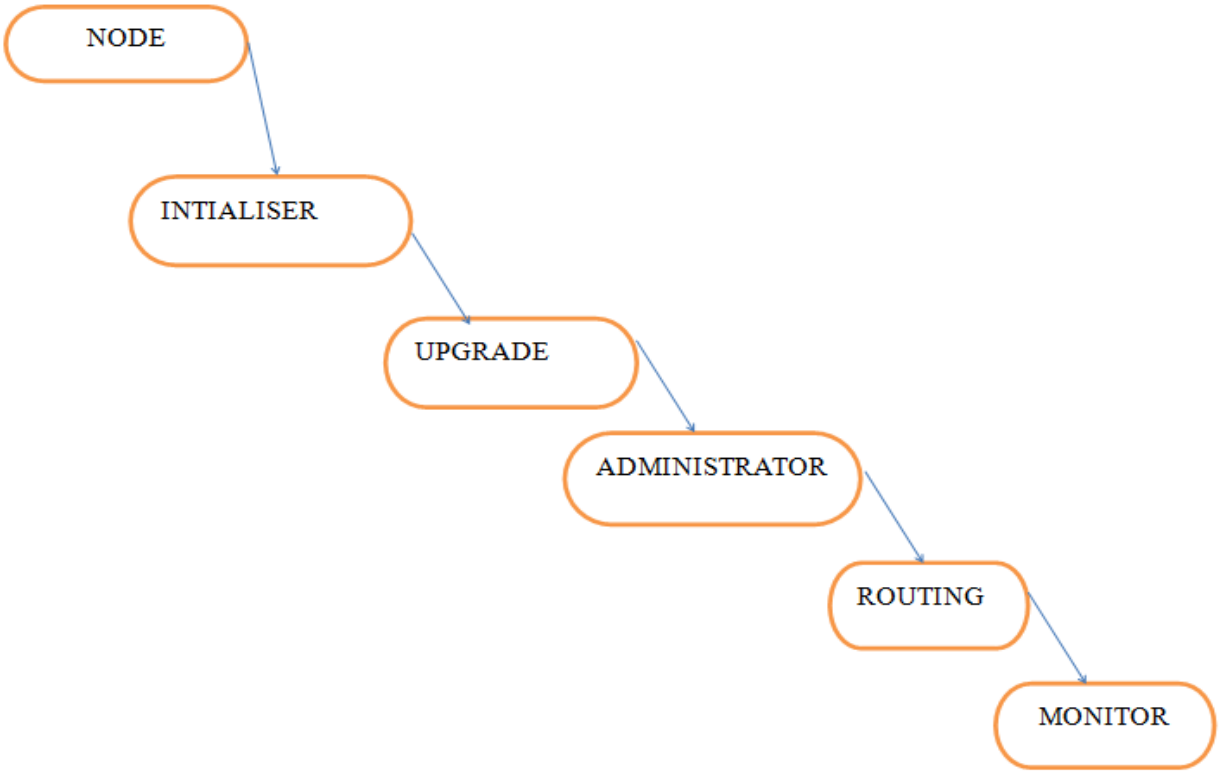
ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

LEVEL 2



IX. TESTING AND IMPLEMENTATION

PERFORMANCE EVALUATION

A discrete event simulator NS2 is used to simulate proposed algorithm. In simulation, the channel capacity of mobile hosts is set to thesame value: 2 Mbps. The distributed coordination function (DCF) of IEEE 802.11 for wireless LANs as the MAC layer protocol. It has the functionality to notify the network layer about link breakage.

In simulation, mobile nodes move in a 1000 meter x 1000 meter square region for 50 seconds simulation time. Each node assumedto move independently with the same average speed. All nodes have the same transmission range of 250 meters.

No. of Nodes	20,40,60,80 and 100
Area Size	1000 X 1000
Mac	802.11
Radio Range	250m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512
Mobility Model	Random Way Point
Attackers	10% of the nodes
Speed	10,20,30,40,50m/s
Pause time	5

Simulation settings and parameters of EDCA over TCLS and RSRP

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

X. CONCLUSION AND FUTURE WORK

In this research work, a trust based cross layer security protocol is developed for authentication. It includes trust based packet forwarding scheme which is designed for detecting and isolating the malicious nodes using the routing layer information. It uses trust values to favor packet forwarding by maintaining a trust counter for each node. If the trust counter value falls below a trust threshold, the corresponding intermediate node is marked as malicious. Link – layer security using the CBC-X mode is utilized for authentication ,encryption and decryption. By extending work on trust counters by using a certificate authority to provide integrity of network along with resisting attacks from outside.

REFERENCES

1. Amitabh Mishra, “Security and quality of service in ad hocwireless networks ” Cambridge university press, ISBN 978- 0-521-87824-1, 2008
2. Prasant Mohapatra and Srikanth Krishnamurthy, “ad hoc networks:technologies and protocols”, springer , ISBN 0- 387-22689-3, 2005.
3. Farooq Anjum and Petros Mouchtaris, “ Security for wireless ad hoc network ”, john willy and sons, ISBN 978-0-471- 75688-0, 2007
4. Akbani R., Korkmaz T. and Raju G, “HEAP: A packet authentication scheme for mobile ad hoc networks”, Ad Hoc Networks vol 6, issue :7, p.p - 1134-1150, 2008.
5. D. Kim, J. Garcia and K. Obraczka (2003), “Routing Mechanisms for Mobile Ad Hoc Networks based on the Energy Drain Rate”, IEEE Transactions on Mobile Computing. Vol.2, No. 2, 2003, pp.161-173.
6. H. Miranda and L. Rodrigues (2002), “Preventing selfishness in open mobile ad hoc networks”, in Proc. of the Seventh CaberNet Radicals Workshop, pp.1-11.
7. S. Marti, T. Giuli, K. Lai, and M. Baker (2000), “Mitigating routing misbehavior in mobile ad hoc networks”, In Proc. of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom), pp.1-11.
8. L. M. Feeney and M. Nilsson (2001), “Investigating the energy consumption of a wireless network interface in an ad hoc networking environment", In IEEE INFOCOM, pp.1-10.
9. M. Jakobsson, J.P. Hubaux, and L. Buttyan (2003), “A micropayment scheme encouraging collaboration in multi-hop cellular networks”, In Proc. of Financial Crypto 2003, pp.1-19.
10. L. Buttyan and J-P. Hubaux, “Security and cooperation in wireless networks”, available at http://secowinet.ep.ch/.
11. Johnson, D (1994), “Routing in Ad Hoc Networks of Mobile Hosts”, Proc. of the Workshop on Mobile Computing Systems and Applications, pp. 158-163.
12. Perkins, C., and Royer, E. (1999), "Ad hoc On-Demand Distance Vector Routing", Proc. of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, pp. 90-100.