International Journal of Future Generation Communication and Networking
Vol. 4, No. 2, June, 2011

Middleware Services for Security in Scalable and Non-Scalable Heterogeneous Nodes of MANETs

Chandrakant N, Deepa Shenoy P and Venugopal K R
Department of Computer Science and Engineering
University Visvesvaraya College of Engineering
Bangalore University, India
nadhachandra@gmail.com

L M Patnaik
Vice Chancellor
Defence Institute of Advanced Technology, India

Abstract

A mobile ad hoc network (MANET) is a system of wireless mobile nodes with routing capabilities, any group of them capable of forming an autonomous network that requires no infrastructure and is capable of organizing itself into arbitrary changeable topologies. A MANET needs a special mechanism to bear with its ad hoc behaviour. In this paper, we are considering a set of heterogeneous nodes in MANETs, which are having different packet size, different security mechanisms and different communication speed etc. The architecture we propose comprises of two main building blocks, namely security management and communication management across all heterogeneous nodes in the scalable and non scalable MANETs. In this network each node does not understand security techniques of each other nodes, because, there could be different encryption techniques, packet size, protocol etc, hence this network is fully dependent on middleware of MANETs. The proposed solution provides security solutions in middleware for scalable and non scalable MANETs and it has found that the malicious node would not be a part of communication in the network through simulation. This technique is very effective for security issues in heterogeneous nodes in MANETs.

1: Introduction

A MANET rely on the cooperation of all the participating nodes that makes dynamic changes in topology and in the availability of resources from different sources. Different sources can be of Laptops, PDAs, Desktops, mobile phones etc. A middleware generalizes the concept of collaborating among these different kinds of devices as shown in Fig 1. This paper is focussing on the point to develop middleware services that provide services for security and communication in mobile adhoc networks, because it is very important to secure the communication between nodes. Middleware is a software infrastructure [9] that bonds together the applications, network hardware, operating systems, and network stacks. The main services of middleware are to provide standardized system services to diverse applications. It provides a runtime environment that can support and coordinate multiple applications. However the main important mechanism of middleware is to achieve adaptive and efficient utilization of resources. A middleware in MANETs has extended its applications communication to a broad set of services supporting a huge spectrum of networked and distributed computing environments. At the same time MANET have become a popular distributed environment and its application domain is expanding rapidly. However, like all distributed environments several issues must be considered and many problems have to be addressed to have efficient and useful applications. Current trends have moved towards using middleware to provide solutions to security, scalability, heterogeneity, resource

Figure 1. Structure of Heterogeneous nodes in MANETs

management and other issues. This paper talks about scalable and non scalable MANETs, scalability is ability to handle growing amount of nodes in the network. Scalability of ad hoc network has been one of the significant areas of the research field. Most of the research works in ad hoc network focus on routing and medium access protocols and produce simulation results for a network size of 50 to 500 nodes. Network scalability is directly related to routing protocols and scalability of DSR, AODV, and LAR routing protocols.

In this paper, we first give a brief overview of security and middleware survey in related work in section 2, we discussed Middleware Challenges For MANETs in section 3. Problem definition has been highlighted in section 4. In section 5 and 6, our design of security concept is described for scalable and non scalable networks in detail. In Section 7, we have shown implementation results and analysis, in this section we have discussed the results and provided information on the configuration of variable parameters. We have simulated ad hoc networks that use our architecture in order to demonstrate its feasibility and to measure performance and overhead. Those measurements are based upon different security models which are described in this section as well. An important contribution of our work is the evaluation of the security architecture has been analysed in this section too. Finally, section 8 concludes the paper and gives an outlook to further research.

2: Related work

Many middleware solutions have been proposed for distributed systems, generally with heavy computational load often adapting synchronous communication style. These approaches are more suited for constant distributed systems since devices are resources rich and high steady bandwidth is assured by the wired links. Example of such approach is: Object Oriented middleware such as CORBA [13],Microsoft COM [15], etc.

The Context Toolkit [6] supports the development of context-aware applications using context widgets with different responsibilities that provide context [5] information to applications. The lowest level interfaces to a physical sensor. The middle layer is concerned with abstracting and combining data. The highest level coordinates the underlying components and provides the callback interface to applications.

The Web Architectures for Service Platforms (WASP) [19]was designed to support context-aware applications specifically in the 3G environment using Web Services technologies and WASP Subscription Language (WSL) to communicate with the platform that connects context-aware applications with context providers (sensors) and third party service providers. The project ”Context Recognition by User Situation Data Analysis (Context)” [20] studies characterization and analysis of information about users’ context and use it in adaptation.

Mires [17] propose an adaptation of a message oriented middleware for traditional fixed distributed systems. Mires provide an asynchronous communication model that is suitable for WSN applications, which

are event driven in most cases, and has more advantages over the traditional request-reply model. It adopts a component-based programming model using active messages to implement its publish-subscribe-based communication infrastructure.

In [21], author has reviewed the state of the art in mobile ad hoc networks security and then identified the security solutions that are relevant for further discussion. The work results in a conceptual security architecture. However, this document does not define the security solutions to be used in tactical mobile ad hoc networks.

In [8] and [7], papers highlights different middleware approaches specifically adopted for wireless mobile ad hoc networks and issues involved and also they tried to clarify some of the ambiguities of middleware definitions. Then they identified the major challenges that the design and development of middleware for MANETs faces.

MaDMAN [12] middleware architecture that enables an adaptive communication infrastructure in mixed delay-tolerant and mobile ad hoc networks. To handle and take advantage of the changing operating conditions that applications in these dynamic environments experience, MaDMAN enables the intelligent exchange of the protocol stacks that implement a communication session in the middle of an ongoing session.

The goal of [3] is to define a middleware providing high-level support for MANET application developers exploiting P2P technology over mobile ad hoc networks. In [11], authors have presented the design of a middleware for mobile ad hoc networks named Transhumance. It aims to support peer-to-peer applications on MANETs with a particular interest in data sharing.

In [10], shows the analytical model for computation of end-to-end delay experienced by a packet when transmitted in an Ad hoc network in which the IEEE 802.11 DCF is used at the MAC layer.

EMID [4] proposes an energy efficient middleware service for wireless sensor network. The proposed algorithm has shown the increase in the network lifetime by computing the essence of each node based on the raw information provided by each sensor node in the network.

Paper [1] reviews the characteristics of each different classes of routing protocols. Moreover, most of current routing protocols assume homogeneous networking conditions where all nodes have the same capabilities and resources. Although homogeneous networks are easy to model and analysis, they exhibits poor scalability compared with heterogeneous networks that consist of different nodes with different resources. And paper also presents extensive studies simulations for DSR, AODV, LAR1, FSR and WRP in homogeneous and heterogeneous networks. The results showed that these which all protocols perform reasonably well in homogeneous networking conditions, their performance suffer significantly over heterogeneous networks. In [2], framework stated the need for novel hybrid approaches to ad hoc routing in order to provide scalability in MANETs [14]. In [18], author have made a performance comparison of seven different mobile ad-hoc routing protocols with respect to various network sizes in homogeneous and heterogeneous networks.

3: Middleware Challenges For MANETs

The successful design and development of a middleware layer for MANETs is to deal with many challenges dictated by the MANET characteristics on one hand and the applications requirements on the other hand. The major challenges are briefly explained here,

SECURITY: As long as communication among hosts in a hostile environment is a primary concern, MANETs poses various challenges to the security design such as open peer-to-peer (P2P) network architecture, a shared wireless medium and a highly dynamic topology. These challenges elevated the prerequisite of developing secure solutions that achieve wider protection at the same time as maintaining desirable network performance. There is no standard security mechanism in a MANET from the security design point of view to address this issue.

HETEROGENEITY: The middleware should offer stumpy level programming models to meet the most important challenge of bridging the gap between hardwares raw possible and the needed activities. It should institute system-level mechanisms interfacing to the different types of hardware and network systems. This will support a broad range of applications and hardware platforms.

QUALITY OF SERVICE: A significant and exclusive property of middleware for MANETS is dictated by the design principles of application understanding. On the other hand, middleware has to include mechanisms

for infusing application understanding in the infrastructure of the network. This allows mapping application communication necessities to network parameters for fine-tuning the network supervising process. Nearly everyone ad hoc network applications dictate minimum quality of service (QoS) necessities sustained over an extended period of time. Middleware should be able to support QoS and dynamically regulate to changes in QoS requirements.

LIMITED RESOURCES: Middleware should supply mechanisms for efficient use of processing, memory and communication resources, at the same time as maintaining low power consumption. A node should accomplish its basic operations without resources overtiredness. As an example of energy aware middleware, most of the devices components as well as the transceivers should be automatically turned on and off based on the application necessities.

SCALABILITY: If a network application gets larger, the network should be bendable enough to allow the addition of more nodes anywhere any time without upsetting the network performance. Proficient middleware services must be capable of maintaining satisfactory levels of performance, as the network grows bigger.

CONTEXT AWARENESS: Context means every portion that can bang the behaviour of an application; therefore the middleware should be context responsive. We can make a distinction two types of awareness: device awareness and environment awareness. Device awareness relates to the domestic resources of the device: battery power, processing power, and memory. Environment awareness relates to exterior resources around the device such as network connectivity, bandwidth, location, and other hosts in variety.

MOBILITY AND NETWORK TOPOLOGY: Due to the self-motivated nature of a MANET, it shows signs of frequent and unpredictable topology changes. The mobile nodes dynamically establish routes between themselves as they move; moreover a user in a MANET may not only operate within the ad-hoc network, but may also necessitate access to a public fixed network. Therefore MANETs should be able handle the traffic and propagation conditions to the nodes mobility patterns.

4: Problem Definition

One of the key tasks of a MANET is their ability to bridge the gap between the physical and logical worlds by gathering certain useful information from the physical world and communicating that information to more powerful logical devices that can process it. The lifetime of MANET is limited due to lack of battery power also it has some additional limitations like resources e.g memory. There is one more important issue in MANETs i.e., security. Due to the absence of a clear line of defense, a complete security solution for MANETs should integrate both proactive and reactive approaches. The solution should comprise of all three components: prevention, detection and reaction. The objective of this paper is to secure the network communication among heterogeneous nodes by applying Middleware concepts.

4.1 Assumptions

We have assumed below parameters for this paper. All nodes are heterogeneous devices in nature, that means each node consists of dissimilar or diverse functionality w.r.t security techniques, packets etc.
Each node cannot send/receive packets from other nodes or neighbours other than base/header node.
This network is fully dependent on middleware services for MANETs.
This paper considered only communication failure due to malicious(L) node(s) entry into the network.

5 Security in Non-Scalable Heterogeneous MANETs

In this section we have assumed that, given network is not growing any more and number of nodes are fixed in the nature. Table 1 enlists all variables used across this paper. We have assumed that MANET is a set of heterogeneous nodes called h_1, h_2...h_n as specified in equation (1), where H is a set of h_1, h_2, ... h_n.

$$H = \{ h_1, h_2,...h_n \} \quad (1)$$

Table 1. System Parameters Definitions

Parameter	Definitions
N	Number of nodes in the network
L	Malicious node in the network
M	Middleware
H	Heterogeneous Node
P	Probability
S	Security Technique
$R1$	Request
$R2$	Response
Mk	Base Node with ***M***
d	Delay
T	Total Time Without *Mk*
ack_L	acknowledgement for L

where each node is having different security techniques i.e.,h_1 is having a security technique called s_1 and so on, therefore equation (2) shows, *S* is a set of security techniques of all heterogeneous nodes.

$$S = \{\ s_1, s_2 ... s_n\ \} \tag{2}$$

here *H* and *S* are having one to one relationships. Here also s_1,s_2...s_n can have sub security techniques called e_1,e_2...e_n. One important note is, in this network each node does not understand security techniques of other nodes because of their own encryption techniques etc, hence this network is fully dependent on middleware of MANETs. The Encryption functionality can include a set of security functions to encrypt, decrypt and sign applicative data,ensuring confidentiality and integrity.

There is a maximum *N(N-1)* bidirectional communication link can happen between nodes with using a header node (*Mk*) who is placed with a middleware software called *M*. The Middleware is an one stop solution for security in communication model as shown in Fig 2. Integration modulation($i_1..i_m$) is the process of linking together different secured nodes (n_1,n_2...n_m) and software applications functionally to act as a coordinated whole. Therefore, *M* in *Mk* is set of integration modules is given in equation (3),

$$M = \{\ i_1 + i_2 ... i_m\ \} \tag{3}$$

Each node's request or response has to reach *Mk*, then *Mk* will process it and delivered to the intendant node(s). As described in earlier paragraph, say security technique s_1 and s_2 is given in equation (4),

$$P(\ s_1 \textit{ and } s_2) = 0 \text{ (disjoint)} \tag{4}$$

As all nodes are heterogeneous in nature, hence we have assumed that $s_1 \neq s_2 \neq s_3 \neq ... s_n$.

Say node n_1 wants to send a request R_1 to the node n_2, equation (5) shows the process, here every node has to send their request or response through *Mk*.

$$n_1 \longrightarrow n_2 = n_1 \rightarrow Mk + Mk \rightarrow n_2 \tag{5}$$

and node n_2 sends a response R_2 back to the node n_1, equation (6) shows the reverse process of equation (5).

$$n_2 \longrightarrow n_1 = n_2 \rightarrow Mk + Mk \rightarrow n_1 \tag{6}$$

Here *Mk* is an intermediate node with M which does integration between all nodes in the network. Basically it does mappings and conversions across the network as shown in Fig 3. The operations of *Mk* could be request-response handling, parameters mapping, protocol management and packet management etc. Fig 3 and Fig 4 shows one to one and many to many communication links through *Mk* respectively.

This kind of network may suffer from communication failures such as, Middleware failure or entry of Malicious nodes or network energy lost or natural disaster etc. The Middleware failure can occur due to non supportive security technology or invalid request/response from nodes.

In this paper, we have considered communication failure due to malicious(*L*) node(s) entry into the network. However *L* cannot communicate with other nodes directly, hence this node has to contact *Mk* for

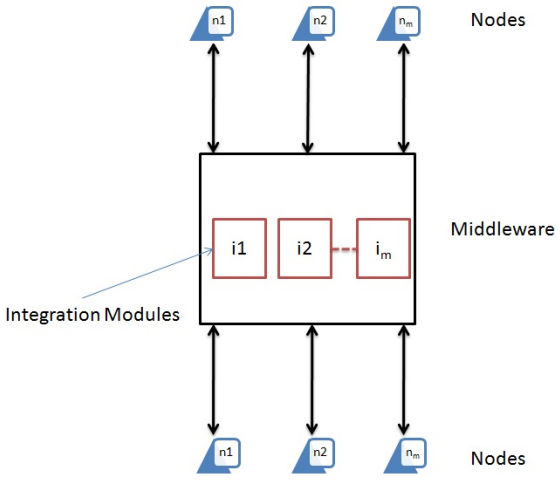

Figure 2. General Middleware Architecture

request and response. Say node *L* wants to send a request R_1 to node n_1, equation (7) shows the process of sending a request to *Mk*,

$$L \longrightarrow n_1 = L \rightarrow Mk + Mk \rightarrow n_1 \qquad (7)$$

Mk does not forward R_1 to n_1, instead *Mk* will validate the request whether this node is registered in *Mk*'s registry or not. Moreover, integration should support for this request/response technically but this is not the case in this scenario. If it is a registered node then it forwards request to node n_1 asks for validity of node *L* for the first time. Then again n_1 will check the genuinity of the same and reply back to *Mk* if it is genuine node or sends acknowledgement(ack_L) packet to *Mk* if it is malicious node.

As we are using intermediate technology (i.e., *M*), the request/response can be delayed due to processing time, mapping time or conversion time etc. The estimation of packet end-to-end delay depends on that of one-hop packet delay. Basically, this delay is the interruption from the moment a packet reaches the head of the queue to the time the sender knows the packet is fruitfully received through the reception of an acknowledgement. The expression of MAC delay gives average service time of a packet in a node. It consists of three parts:

- Time to transmit packet successfully once
- Total time a node spends in back off
- Total time spent by *Mk*
- Total transmission time used for retransmission of the packet

The analysis of delay by *Mk* is derived a in equation (8),

$$\mathrm{d}(\, n_1 \longrightarrow n_2\,) = T = \mathrm{d}(\, n_1 + n_2\,) \qquad (8)$$

using *Mk* for communication in equation (9),

$$\mathrm{d}(\, n_1 + Mk + n_2\,) = \mathrm{d}(T+\delta) \qquad (9)$$

here, δ is delay by *Mk* as given in equation (10),

$$Mk = \delta \qquad (10)$$

Overall delay is calculated in equation (11),

$$\delta = \mathrm{d}(\text{Evaluating } s_1 \text{ or } s_2 \text{ or } s_3 \ldots s_n) + \mathrm{d}(\text{mappings/conversion}) \qquad (11)$$

using equation (8) and (9) we have arrived to equation (12),

$$\mathrm{d}(\, n_1 + n_2\,) = T \qquad (12)$$

6 Security in Scalable Heterogeneous MANETs

This section is continuation of previous section except the concept of network growth. Scalability is the ability of a system, network or process, to handle growing amounts of work in a graceful manner or its capability to be enlarged to accommodate that growth. As given in paper [4], scalability is defined as, the ability of a routing protocol to perform efficiently as one or more inherent parameters of the network grow to be large in value.

As network grows, we need to have many *Mk* systems to accommodate the incoming nodes. Say *n* is the maximum number of nodes managed by a middleware system Mk_1. Therefore,

$$Mk = \{\ Mk_1, Mk_2, Mk_3 ... Mk_n\ \} \qquad (13)$$

Let us see Integer Linear Programming model[16], say *N* be the set of nodes of a network which is assigned to a middleware system. The physical distance between two nodes n_1, $n_2 \in N$ is given by $d_{n_1,n_2} \in R^+$ and parameter $d^{max} \in R^+$ represents a maximum allowed distance between intra-*Mk*'s nodes. We denote the decision variables that determine whether a node $n \in N$ is contained in a registry of middleware system Mk_1 $\in$ *Mk* by $X_{Mk_1,n} \in 0, 1$. The variables $Y_{Mk_1,n_1,n_2} \in R_0^+$ reveal whether nodes n_1, $n_2 \in N$ are situated in the same registry of middleware system $Mk_1 \in Mk$. The mathematical model is then given by the following equations.

$$\text{Minimize} \sum_{\substack{Mk_1 \in Mk \\ \{n_1,n_2\} \subset N}} Y_{Mk_1,n_1,n_2}.d_{n_1,n_2} \quad (14)$$

The objective of equation(14) minimizes the total sum of the distances between all nodes that are included in the same Mk1 i.e., individual middleware system. For this we consider all node pairs $\{n_1, n_2\} \subset N$, i.e. all unsorted node subsets consisting of two distinct nodes $n_1, n_2 \in N$. By doing so, the distance between two nodes will be counted only once as opposed to twice if dealing with ordered 2-tupels. Subject to,

$$\sum_{Mk_1 \in Mk} X_{Mk_1,n} = 1 \quad \forall n \in N \qquad (15)$$

Here *n* is the size of nodes existed in Mk_1. The objective of equation(15) guarantee that every node *n* is included in exactly one middleware system Mk_1.

$$Y_{Mk_1,n_1,n_2} \geq X_{Mk_1,n_1} + X_{Mk_1,n_2} - 1\ ; \forall Mk_1 \in Mk, \forall \{n_1, n_2\} \subset N \qquad (16)$$

Equation (16) provides a lower bound based on the middleware system allocation variables for each node in order to be able to distinguish node pairs that are assigned to the same middleware system. The right side of the equation will equal one, only if both considered nodes are in the identical network head by middleware system.

$$Y_{Mk_1,n_1,n_2} = 0\ ; \forall Mk_1 \in Mk, \forall \{n_1, n_2\} \subset N : d_{n_1,n_2} \gg d^{max} \quad (17)$$

$$X_{Mk_1,n} \in \{0, 1\}, Y_{Mk_1,n_1,n_2} \in R_0^+ \qquad (18)$$

Equations (17) and (18) are optional constraints which reduce the solution space and are motivated by the goal of the *Mk* strategy at the same time. An efficient configuration integrates nodes in one *Mk* in case they are situated close to each other to reduce the sum of the node distances. Thus, it is very likely that nodes far away from each other are put into distinct *Mk*s. The equation prohibits nodes to be in the same network partition as soon as their distance exceeds a maximum value d^{max}.

Say node *Q* enters into a network which is controlled by Mk_1, however as soon as a node enters into a network it cannot communicate with other nodes directly or indirectly unless Mk_1 approves of indirect communication, hence this node has to contact Mk_1 for authentication. Now Mk_1 will validate the genuinity of *Q*, if *Q* is not a malicious node then it approves for communication through itself. But there is a issue w.r.t compatibility of communication protocol and techniques, hence Mk_1 has to integrate or build the interface for a node *Q* and make a entry into Mk_1's registry then *Q* can start communicating with Mk_1. Building an interface or integration for any node has to consider a new (probably) security technique(s) of new node etc.

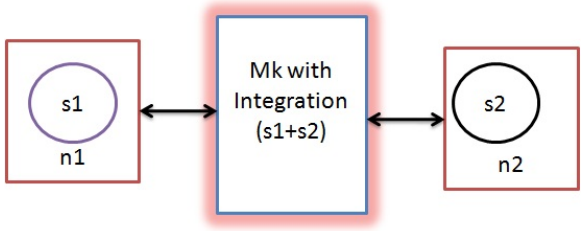

Figure 3. Nodes communication through middleware-one to one

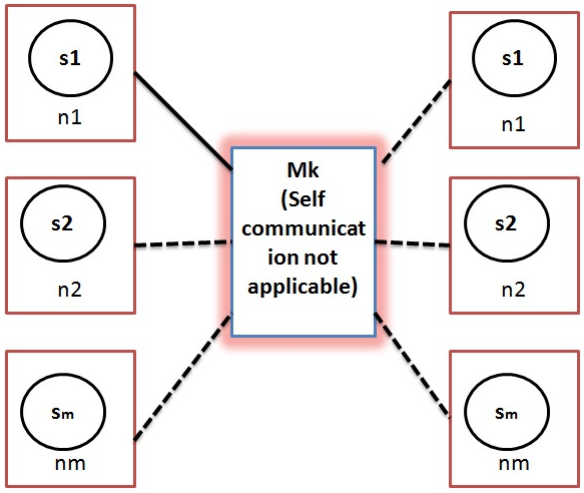

Figure 4. Nodes communication through middleware-many to many

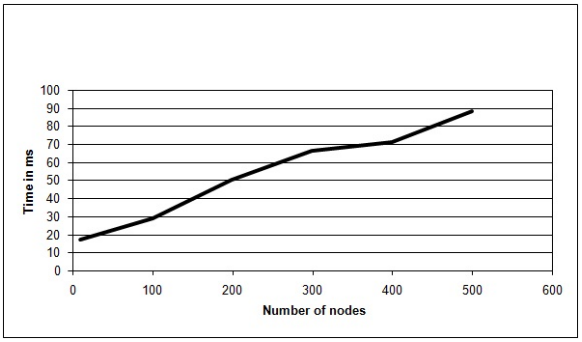

Figure 5. Average Request/Response Delay by Mk With 50% Malicious Nodes (Non-Scalable)

Say node Q wants to send a request R_1 to node n_1, equation (19) shows the process of sending a request to Mk_1,

$$Q \longrightarrow n_1 = Q \rightarrow Mk_1 + Mk_1 \rightarrow n_1 \quad (19)$$

Mk_1 does not forward R_1 to n_1, instead Mk_1 will validate the request whether this node is registered in Mk_1's registry or not. If it is a registered node then it forwards request to node n_1 asks for validity of node Q for the first time. Then again n_1 will check the genuinity of the same and reply back to Mk_1 if it is genuine node or sends acknowledgement(ack_Q) packet to Mk_1 if it is malicious node.

7 Implementation

This section shows the overview of simulation of ad-hoc network communication. This work has been carried out using JAVA. The most important class of the project is *Manets*. It keeps all other parts collectively and gets everything to work. This is where the main method of the whole project is located. This also includes starting the client applications. *Middleware* class consisting of communication services, e.g., transferring requests. *Node* class specifies all properties of nodes. Additional classes exist for utility and supporting purpose.

7.1 Experiment Results and Analysis

We have started experimenting by taking 500 nodes in scalable/non-scalable MANETs. We have calculated the time delay with malicious nodes as shown in Fig 5 and without malicious nodes as shown in Fig 6. The graph shows the statistics of the network by using middleware techniques in heterogeneous network. In our experiment, we have considered 50% malicious nodes, due to security by *Mk*, almost all nodes are neglected, hence entire channel is available for request/response for genuine nodes, therefore performance is better in Fig 5 compared to Fig 6. We also experimented scalable MANETs as shown in Fig 7, there are 5 base nodes called (Mk_1,Mk_2,Mk_3,Mk_4 and Mk_5), each base node will have a set of children nodes varies from 100 to 500, therefore this network is dynamically growing over a period and showing the request/response time.

8 Conclusions

Security solutions are very important for heterogeneous nodes in MANETs as these networks are more vulnerable to hackers or crackers. We have discussed and proposed potential enhancements and new research possibilities in middleware. It is important to mention that designing and implementing the middleware that fully meets all the requirements and challenges of a mobile ad hoc environment and incorporate various

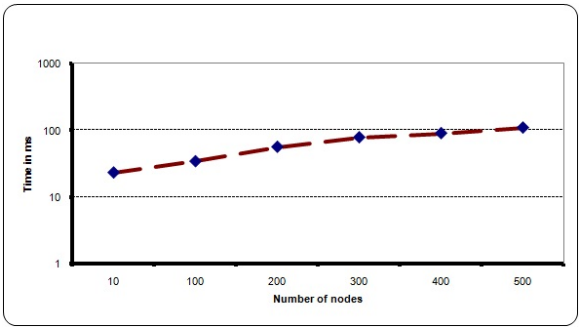

Figure 6. Average Request/Response Delay by Mk Without Malicious Nodes(Non-Scalable)

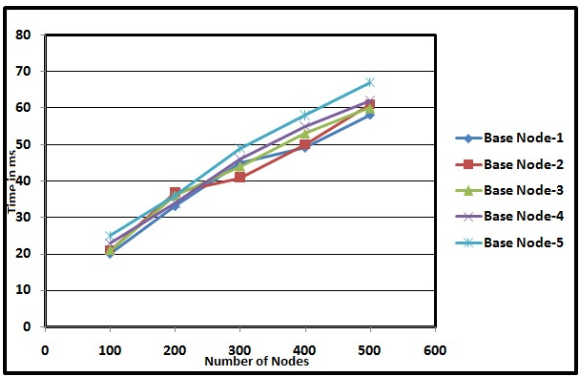

Figure 7. Average Request/Response Delay by each Mk Without Malicious Nodes (Scalable)

techniques and methodologies that will proved as much of the required functionality as possible, while maintaining flexibility, efficiency and scalability. In this paper we have proposed a solution to security solutions in middleware for scalable and non scalable MANETs and it has found that the malicious node would not be a part of communication in the network. This technique is one of the effective technique for security issues in heterogeneous nodes in MANETs. The future enhancement could be, evaluation of middleware failures, single point failure and managing the same.

References

[1] H. A. Amri, M. Abolhasan, and T. Wysocki. Scalability of manet routing protocols for heterogeneous and homogenous networks. In *Telecommunication and Information Research Institute, University of Wollongong, Wollongong, NSW 2522, Australia*.

[2] E. Baccelli and J. Schiller. Towards scalable manets. In *LIX - Ecole Polytechnique,91128 Palaiseau Cedex, FRANCE*.

[3] M. Bisignano, A. Calvagna, G. D. Modica, and O. Tomarchio. Expeerience: a jxta middleware for mobile ad-hoc networks. In *Proceedings of the Third International Conference on Peer-to-Peer Computing (P2P 2003)*.

[4] N. Chandrakant, H. Deshpande, J. Tejas, P. D. Shenoy, K. R. Venugopal, and L. M. Patnaik. Emid: Maximizing lifetime of wireless sensor network by using energy efficient middleware service. In *2011 International Conference on Intelligent Information Networks, ICIIN 2011*, Mar 2011.

[5] G. Chen and D. Kotz. Solar: A pervasive-computing infrastructure for context-aware mobile applications. Technical report, Department of Computer Science, Dartmouth College, Hanover, NH, USA, Feb 2002.

[6] A. K. Dey, D. Salber, and G. D. Abowd. A conceptual framework and a toolkit for supporting the rapid prototyping of contextaware applications. In *Human-Computer Interaction (HCI) Journal*, volume 16, pages 97–166, 2001.

[7] S. Hadim, J. Al-Jaroodi, and N. Mohamed. Middleware issues and approaches for mobile ad hoc networks. In *In proc. of IEEE Consumer Communications and Networking Conference (CCNC 2006), Las Vegas, Nevada, January 2006*.

[8] S. Hadim, J. Al-Jaroodi, and N. Mohamed. Trends in middleware for mobile ad hoc networks. In *JOURNAL OF COMMUNICATIONS, VOL. 1, NO. 4, JULY 2006*.

[9] A. Kumar, P. Gupta, P. K. Verma, and V. Lamba. Concept of middleware services in mobile ad-hoc networks. In *International Journal of Computer Applications (0975 8887) Volume 2 No.8, June 2010*.

[10] R. Kumar, M. Misra, and A. K. Sarje. A simplified analytical model for end-to-end delay analysis in manet. In *IJCA Special Issue on Mobile Ad-hoc Networks MANETs, 2010*.

[11] G. Paroux, L. Martin, J. Nowalczyk, and I. Demeure. Transhumance: A power-sensitive middleware for data sharing on mobile ad hoc networks. In *France Telecom R and D, 38-40 avenue du Gnral Leclerc, 92 130 Issy- Les-Moulineaux, France,2007*.

[12] A. Petz, A. Bednarczyk, N. Paine, D. Stovall, and C. Julien. Madman: A middleware for delay-tolerant mobile ad-hoc networks. In *TR-UTEDGE-2010-011*.

[13] A. Pope. The corba ref. guide: Understanding the common object request broker architecture. Technical report, Addison-Wesley, and Jan. 1998.

[14] A. Post. Towards a scalable ad hoc network infrastructure. In *Rice University, Houston, TX, USA*.

[15] D. Rogerson. Inside com. Technical report, Microsoft Press, 1997.

[16] M. Scheffel, M. Kiese, and T. Stidsen. A clustering approach for scalable network design. In *German Ministry of Education and Research under the Project ID 01BP551*.

[17] E. Souto, G. Guimares, G. Vasconcelos, M. Vieira, N. Rosa, and C. Ferraz. A message-oriented middleware for sensor networks. In *Proc. 2nd Int"l Workshop Middleware for Pervasive and Ad-Hoc Computing (MPAC 04),ACM Press*, pages 127–134, 2004.

[18] T. Sundararajan, Karthik, and A. Shanmugam. Security and scalability of manet routing protocols in homogeneous and heterogeneous networks. In *Proceedings of the International Conference on Man-Machine Systems (ICoMMS) 11 13 October 2009, Batu Ferringhi, Penang, MALAYSIA*.

[19] I. Telematica. Web services: the cement for mobile, context-aware services. Technical report, http://www.freeband.nl/kennisimpuls/projecten/wasp /ENindex.html, May 2004.

[20] F. UNIVERSITY OF HELSINKI. Context recognition by user situation data analysis (context). Technical report, http://www.cs.helsinki.fi/en/contact/, Aug 2010.

[21] O. Winberg. Survey of security solutions for mobile ad hoc networks. In *Frsvarets materielverk 2007*.