International Journal of Enterprise Computing and Business Systems
ISSN (Online) : 2230-8849
Volume 5 Issue 2 July - December 2015
International Manuscript ID : 22308849072015-01

DYNAMIC KEY BASED SECURITY PROTOCOL IN NETWORK COMMUNICATION

Shubham Rathi
M.Tech. Research Scholar
Computer Science and Engineering
Modern Institute of Engineering and Technology
Ambala, Haryana, India
E-mail : shubham.rathi88@gmail.com

Gagan Kumar
Assistant Professor
Computer Science and Engineering
Modern Institute of Engineering and Technology
Ambala, Haryana, India
E-mail : gagansoft@gmail.com

ABSTRACT

Security has turned into an essential concern so as to give secured correspondence between portable hubs in a threatening situation. Not at all like the wired networks, the special qualities of portable impromptu networks represent various nontrivial difficulties to security outline, for example, open shared network construction modeling, imparted remote medium, stringent asset imperatives, and exceptionally element network topology. These difficulties obviously present a defense for building multifence security arrangements that accomplish both expansive insurance and attractive network execution. In this article we concentrate on the crucial security issue of

International Journal of Enterprise Computing and Business Systems
ISSN (Online) : 2230-8849
Volume 5 Issue 2 July - December 2015
International Manuscript ID : 22308849072015-01

ensuring the multihop network integration between versatile hubs in a Wireless Sensor Network. We recognize the security issues identified with this issue, examine the difficulties to security plan, and audit the cutting edge security proposition that secure the Wireless Sensor Network join and network-layer operations of conveying parcels over the multihop remote channel. The complete security arrangement ought to compass both layers, and include each of the three security segments of avoidance, location, and response. Security has turned into an essential concern keeping in mind the end goal to give secured correspondence between versatile hubs in an antagonistic domain. Dissimilar to the wired networks, the interesting attributes of portable specially appointed networks represent various nontrivial difficulties to security configuration, for example, open shared network structural engineering, imparted remote medium, stringent asset imperatives, and exceedingly element network topology. These difficulties plainly present a defense for building multifence security arrangements that accomplish both wide insurance and attractive network execution. In this examination work, we will concentrate on the major security issue of ensuring the adhoc network integration between versatile hubs in a Wireless Sensor Network. We distinguish the security issues identified with this issue, talk about the difficulties to security outline, and survey the best in class security proposition that secure the Wireless Sensor Network join and network-layer operations of conveying parcels over the multihop remote channel. The complete security arrangement ought to compass both layers, and include every one of the three security segments of anticipation, location, and response. In this examination proposition, we propose and implement a novel calculation for security and reliability in wireless networks.

Keywords – Network Security, Dynamic Key Exchange, Network Defense

INTRODUCTION

Wireless Network [1] is defined as the moving node rather than any fixed infrastructure, act as a mobile router. These mobile routers are responsible for the network mobility. The history of mobile network begin after the invention of 802.11 or WiFi [2] they are mostly used for

connecting among themselves and for connecting to the internet via any fixed infrastructure. Vehicles like car, buses and trains equipped with router acts as nested Mobile Ad-hoc Network. Vehicles today consists many embedded devices like build in routers, electronic devices like Sensors PDAs build in GPS, providing internet connection to it gives, information and infotainment to the users. These advances in Wireless Sensor Network helps the vehicle to communicate with each other, at the time of emergency like accident, or during climatic changes like snow fall, and at the time of road block, this information will be informed to the nearby vehicles. Nowadays technologies rising to provide efficiency to Wireless Sensor Network users like providing enough storage space, as we all know the cloud computing is the next generation computing paradigm many researches are conducting experiments on Mobile Ad-hoc Network to provide the cloud service securely.

A mobile ad hoc network (Wireless Sensor Network) is a self-configuring infrastructureless network of mobile devices connected by wireless. Ad hoc is Latin and means "for this purpose".[1]

Each device in a Wireless Sensor Network is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a Wireless Sensor Network is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet.

Wireless Sensor Network s are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network.

International Journal of Enterprise Computing and Business Systems
ISSN (Online) : 2230-8849
Volume 5 Issue 2 July - December 2015
International Manuscript ID : 22308849072015-01

The growth of laptops and 802.11/Wi-Fi wireless networking has made Wireless Sensor Network s a popular research topic since the mid-1990s. Many academic papers evaluate protocols and their abilities, assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other. Different protocols are then evaluated based on measures such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput etc.

In recent years, the explosive growth of mobile computing devices, which mainly include laptops, personal digital assistants (PDAs) and handheld digital devices, has impelled a revolutionary change in the computing world: computing will not merely rely on the capability provided by the personal computers, and the concept of ubiquitous computing emerges and becomes one of the research hotspots in the computer science society [1]. In the ubiquitous computing environment, individual users utilize, at the same time, several electronic platforms through which they can access all the required information whenever and wherever they may be [2]. The nature of the ubiquitous computing has made it necessary to adopt wireless network as the interconnection method: it is not possible for the ubiquitous devices to get wired network link whenever and wherever they need to connect with other ubiquitous devices. The Mobile Ad Hoc Network is one of the wireless networks that have attracted most concentrations from many researchers. A Mobile Ad hoc NETwork (Wireless Sensor Network) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. People and vehicles can thus be internetworked in areas without a preexisting communication infrastructure or when the use of such infrastructure requires wireless extension [3]. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that not in the direct communication range use intermediate node(s) to communicate with each other. In these two situations, all the nodes that have participated in the communication automatically form a wireless network, therefore this kind of wireless network can be viewed as mobile ad hoc network. The mobile ad hoc network has the following

typical features [4]: Unreliability of wireless links between nodes. Because of the limited energy supply for the wireless nodes and the mobility of the nodes, the wireless links between mobile nodes in the ad hoc network are not consistent for the communication participants. Constantly changing topology.

Due to the continuous motion of nodes, the topology of the mobile ad hoc network changes constantly: the nodes can continuously move into and out of the radio range of the other nodes in the ad hoc network, and the routing information will be changing all the time because of the movement of the nodes. Lack of incorporation of security features in statically configured wireless routing protocol not meant for ad hoc environments. Because the topology of the ad hoc networks is changing constantly, it is necessary for each pair of adjacent nodes to incorporate in the routing issue so as to prevent some kind of potential attacks that try to make use of vulnerabilities in the statically configured routing protocol. Because of the features listed above, the mobile ad hoc networks are more prone to suffer from the malicious behaviors than the traditional wired networks. Therefore, we need to pay more attention to the security issues in the mobile ad hoc networks.

Vehicular Ad hoc Networks (VANETs) are used for communication among vehicles and between vehicles and roadside equipment. Internet based mobile ad hoc networks (iWireless Sensor Network s) are ad hoc networks that link mobile nodes and fixed Internet-gateway nodes. In such type of networks normal adhoc routing algorithms don't apply directly. 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, drunken driving etc.

A mobile ad-hoc network (Wireless Sensor Network) is an ad-hoc network but an ad-hoc network is not a Wireless Sensor Network.

International Journal of Enterprise Computing and Business Systems
ISSN (Online) : 2230-8849
Volume 5 Issue 2 July - December 2015
International Manuscript ID : 22308849072015-01

DATA MONITORING AND MINING

Wireless Sensor Network S can be used for facilitating the collection of sensor data for data mining for a variety of applications such as air pollution monitoring and different types of architectures can be used for such applications.[2] It should be noted that a key characteristic of such applications is that nearby sensor nodes monitoring an environmental feature typically register similar values. This kind of data redundancy due to the spatial correlation between sensor observations inspires the techniques for in-network data aggregation and mining. By measuring the spatial correlation between data sampled by different sensors, a wide class of specialized algorithms can be developed to develop more efficient spatial data mining algorithms as well as more efficient routing strategies.[3] Also researchers have developed performance models[4][5] for Wireless Sensor Network by applying Queueing Theory.

A lot of research has been done in the past but the most significant contributions have been the PGP (Pretty Good Privacy) and trust based security. None of the protocols have made a decent trade off between security and performance. In an attempt to enhance security in Wireless Sensor Network s many researchers have suggested and implemented new improvements to the protocols and some of them have suggested new protocols.

ATTACK CLASSIFICATIONS

These attacks on Wireless Sensor Network s challenge the mobile infrastructure in which nodes can join and leave easily with dynamics requests without a static path of routing. Schematics of various attacks as described by Al-Shakib Khan [1] on individual layer are as under:

Application Layer: Malicious code, Repudiation
Transport Layer: Session hijacking, Flooding
Network Layer: Sybil, Flooding, Black Hole, Grey Hole. Worm Hole, Link Spoofing, Link Withholding, Location disclosure etc.

International Journal of Enterprise Computing and Business Systems
ISSN (Online) : 2230-8849
Volume 5 Issue 2 July - December 2015
International Manuscript ID : 22308849072015-01

Data Link/MAC: Malicious Behavior, Selfish Behavior, Active, Passive, Internal External
Physical: Interference, Traffic Jamming, Eavesdropping

In case a mobile node wants to communicate with another mobile node which is too far from the source node, it should depend on relay node as bridge to communicate with destination. Relay node is nothing but another mobile node. In this case there arises a question of security. Apart from authentication, reliability and acceptance it should also aware of the address location and packet traffic digression.

In this work we are going to concentrate on the various issues that affect the ad-hoc networks security mechanism and also we are going to concentrate on pros and cons of Mobile networks protocols. We are also concentrating on enhancing security and reliability to Mobile Ad-hoc Network (Wireless Sensor Network) [1].

Many researches were done before to provide security to Wireless Sensor Network [1] but none of the protocol shines in providing security and performance. There are many defects in the Mobile framework; this may cause unknown nodes to connect frequently without any proper routing. In order to prevent other nodes from trespassing we are going to concentrate on providing more security to Mobile Ad-hoc network.

There were so many research areas in Wireless Sensor Network [1] in that security is the major concern among others.
The scope of securing Wireless Sensor Network [1] is mentioned here

- Securing Wireless Sensor Network s [1] is great challenge for many years due to the absence of proper infrastructure and its open type of network.
- Previous security measures in Wireless Sensor Network s [1] are not effective in the challenging world with advancement in technology.

- Many layers often prone to attacks man in middle attack or multilayer attack, so proposal should concentrate on this layers.
- The proper intelligent approach [3] of securing Wireless Sensor Network s [1] has not yet discovered.
- In this project we are going to concentrate on applying bio inspired intelligence [3] techniques for securing Wireless Sensor Networks.

VULNERABILITIES OF THE WIRELESS NETWORKS

Lack of Secure Boundaries

The meaning of this vulnerability is self-evident: there is not such a clear secure boundary in the mobile ad hoc network, which can be compared with the clear line of defense in the traditional wired network. This vulnerability originates from the nature of the mobile ad hoc network: freedom to join, leave and move inside the network. In the wired network, adversaries must get physical access to the network medium, or even pass through several lines of defense such as firewall and gateway before they can perform malicious behavior to the targets [6]. However, in the mobile ad hoc network, there is no need for an adversary to gain the physical access to visit the network: once the adversary is in the radio range of any other nodes in the mobile ad hoc network, it can communicate with those nodes in its radio range and thus join the network automatically. As a result, the mobile ad hoc network does not provide the so-called secure boundary to protect the network from some potentially dangerous network accesses. Lack of secure boundaries makes the mobile ad hoc network susceptible to the attacks. The mobile ad hoc network suffers from all-weather attacks, which can come from any node that is in the radio range of any node in the network, at any time, and target to any other node(s) in the network. To make matters worse, there are various link attacks that can jeopardize the mobile ad hoc network, which make it even harder for the nodes in the network to resist the attacks. The attacks mainly include passive eavesdropping, active interfering, leakage of secret

information, data tampering, message replay, message contamination, and denial of service [4].

Threats from Compromised nodes Inside the Network

In the previous subsection, we mainly discuss the vulnerability that there is no clear secure boundaries in the mobile ad hoc network, which may cause the occurrences of various link attacks. These link attacks place their emphasis on the links between the nodes, and try to perform some malicious behaviors to make destruction to the links. However, there are some other attacks that aim to gain the control over the nodes themselves by some unrighteous means and then use the compromised nodes to execute further malicious actions. This vulnerability can be viewed as the threats that come from the compromised nodes inside the network. Since mobile nodes are autonomous units that can join or leave the network with freedom, it is hard for the nodes themselves to work out some effective policies to prevent the possible malicious behaviors from all the nodes it communicate with because of the behavioral diversity of different nodes. Furthermore, because of the mobility of the ad hoc network, a compromised node can frequently change its attack target and perform malicious behavior to different node in the network, thus it is very difficult to track the malicious behavior performed by a compromised node especially in a large scale ad hoc network. Therefore, threats from compromised nodes inside the network are far more dangerous than the attacks from outside the network, and these attacks are much harder to detect because they come from the compromised nodes, which behave well before they are compromised.

Lack of Centralized Management Facility

Ad hoc networks do not have a centralized piece of management machinery such as a name server, which lead to some vulnerable problems. Now let us discuss this problem in a more detailed manner. First of all, the absence of centralized management machinery makes the detection of attacks a very difficult problem because it is not easy to monitor the traffic in a highly dynamic and large scale ad hoc network [7]. It is rather common in

the ad hoc network that benign failures, such as path breakages, transmission impairments and packet dropping, happen frequently. Therefore, malicious failures will be more difficult to detect, especially when adversaries change their attack pattern and their attack target in different periods of time. For each of the victims, because it can only observe the failure that occurs in itself, this short-time observation cannot produce a convincing conclusion that the failure is caused by an adversary. However, we can easily find from a system point of view that the adversary has performed such a large amount of misbehaviors that we can safely conclude that all of the failures caused by this adversary should be malicious failure instead of benign failure, though these failures occur in different nodes at different time. From this example we find that lack of centralized management machinery will cause severe problems when we try to detect the attacks in the ad hoc network. Second, lack of centralized management machinery will impede the trust management for the nodes in the ad hoc network [4]. In mobile ad hoc network, all the nodes are required to cooperate in the network operation, while no security association (SA2) can be assumed for all the network nodes. Thus, it is not practical to perform an a priori classification, and as a result, the usual practice of establishing a line of defense, which distinguishes nodes as trusted and nontrusted, cannot be achieved here in the mobile ad hoc network. Third, some algorithms in the mobile ad hoc network rely on the cooperative participation of all nodes and the infrastructure. Because there is no centralized authority, and decisionmaking in mobile ad hoc network is sometimes decentralized, the adversary can make use of this vulnerability and perform some attacks that can break the cooperative algorithm [6].

Security Solutions to the Mobile Ad Hoc Networks

We have discussed several vulnerabilities that potentially make the mobile ad hoc networks insecure in the previous section. However, it is far from our ultimate goal to secure the mobile ad hoc network if we merely know the existing vulnerabilities in it. As a result, we need to find some security solutions to the mobile ad hoc network. In this

section, we survey some security schemes that can be useful to protect the mobile ad hoc network from malicious behaviors.

Availability

The term availability means that a node should maintain its ability to provide all the designed services regardless of the security state of it [4]. This security criterion is challenged mainly during the denial-of-service attacks, in which all the nodes in the network can be the attack target and thus some selfish nodes make some of the network services unavailable, such as the routing protocol or the key management service [5].

Integrity

Integrity guarantees the identity of the messages when they are transmitted. Integrity can be compromised mainly in two ways [9]:

- Malicious altering
- Accidental altering

A message can be removed, replayed or revised by an adversary with malicious goal, which is regarded as malicious altering; on the contrary, if the message is lost or its content is changed due to some benign failures, which may be transmission errors in communication or hardware errors such as hard disk failure, then it is categorized as accidental altering.

Confidentiality

Confidentiality means that certain information is only accessible to those who have been authorized to access it. In other words, in order to maintain the confidentiality of some confidential information, we need to keep them secret from all entities that do not have the privilege to access them.

Authenticity

Authenticity is essentially assurance that participants in communication are genuine and not impersonators [4]. It is necessary for the communication participants to prove their identities as what they have claimed using some techniques so as to ensure the

authenticity. If there is not such an authentication mechanism, the adversary could impersonate a benign node and thus get access to confidential resources, or even propagate some fake messages to disturb the normal network operations.

Nonrepudiation

Nonrepudiation ensures that the sender and the receiver of a message cannot disavow that they have ever sent or received such a message. This is useful especially when we need to discriminate if a node with some abnormal behavior is compromised or not: if a node recognizes that the message it has received is erroneous, it can then use the incorrect message as an evidence to notify other nodes that the node sending out the improper message should have been compromised.

Authorization

Authorization is a process in which an entity is issued a credential, which specifies the privileges and permissions it has and cannot be falsified, by the certificate authority. Authorization is generally used to assign different access rights to different level of users. For instance, we need to ensure that network management function is only accessible by the network administrator. Therefore there should be an authorization process before the network administrator accesses the network management functions.

OBJECTIVES OF THE PROPOSED WORK

- The main objective of the research work is to provide high level security and integrity to the existing systems mainly on the network layer to prevent the attacks etc.
- To investigate and conclude the scope of multi layer attacks.
- To analyze the needs of above mentioned techniques in different network layers especially in the multi link layer.
- To propose a unique technique for different attacks using multilayered hash key.
- Intelligent Wireless Sensor Network proposal to deal with all kinds of attacks.

ISSN (Online) : 2230-8849
Volume 5 Issue 2 July - December 2015
International Manuscript ID : 22308849072015-01

- To validate the techniques by implementing and analyzing its results with the existing systems.

IMPLEMENTATION

The proposed approach is dynamic in nature that makes use of dynamic key exchange. The parallel hybrid approach of md5 and sha1 and implemented for higher security and integrity in the network.

TOOLS / TECHNOLOGIES USED

- MATLAB
- Notepad++

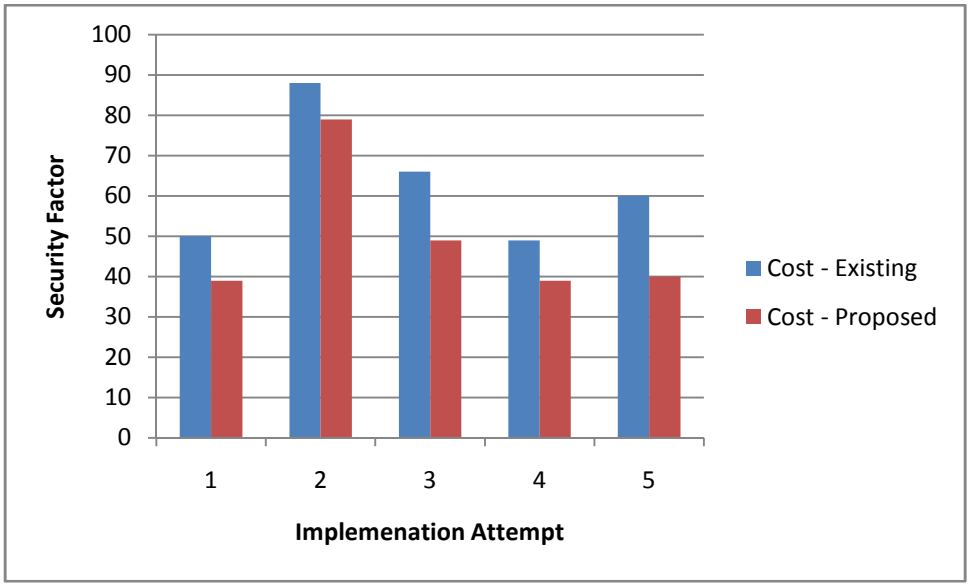
Existing Approach	Proposed Approach
40	60
50	87
44	78
60	89
55	87

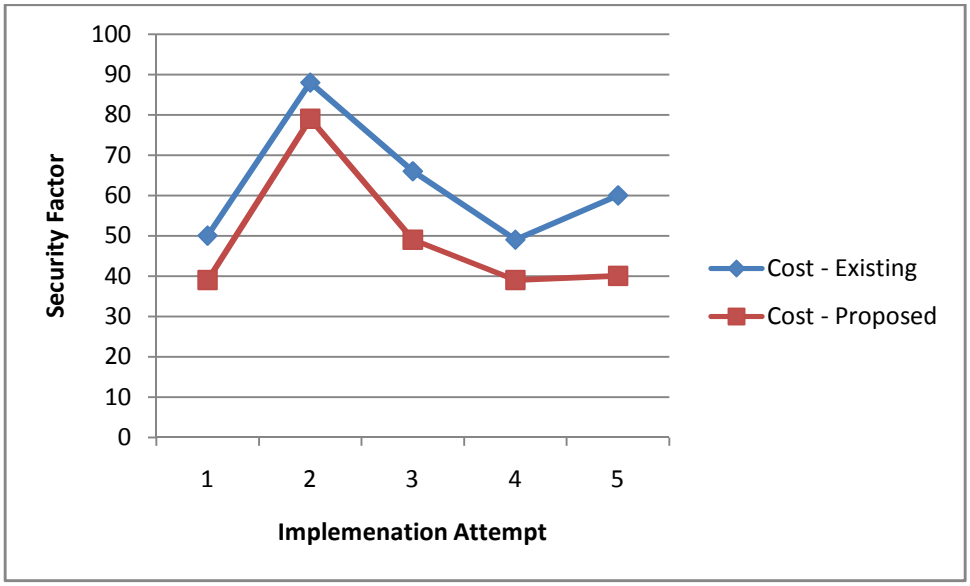
International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

Volume 5 Issue 2 July - December 2015

International Manuscript ID : 22308849072015-01



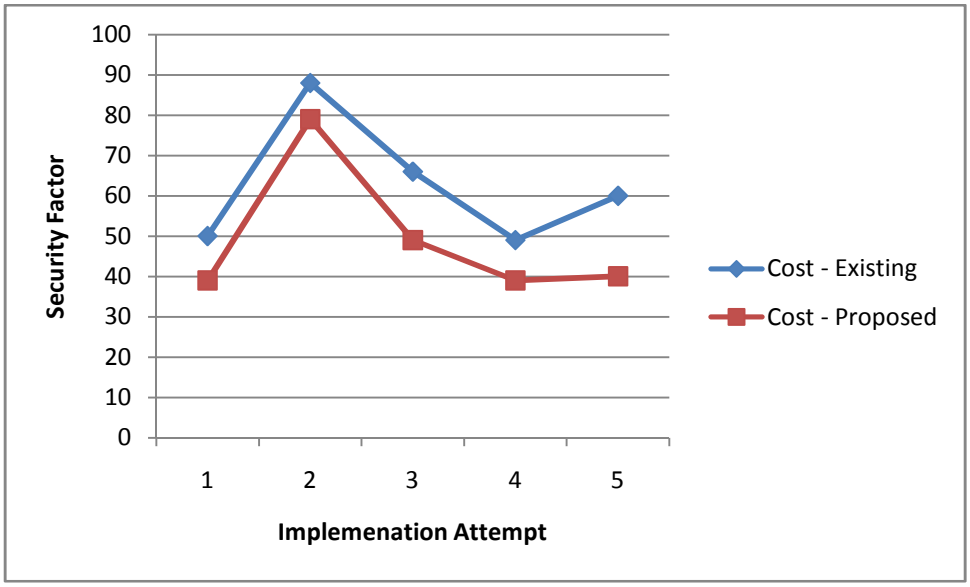


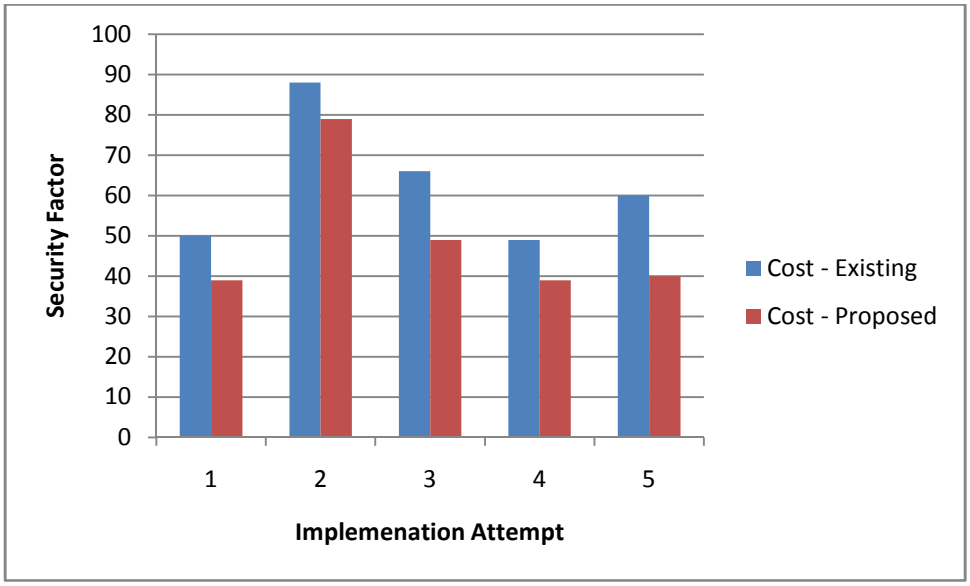
International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

Volume 5 Issue 2 July - December 2015

International Manuscript ID : 22308849072015-01





CONCLUSION

The research work is based on the dynamic key exchange in the wireless and assorted network infrastructure. The results show that the hybrid key based approach in the wireless network is giving better results in terms of higher security and integrity. The proposed and implemented work can be further improved using metaheuristic approaches for the global optimal results.

ISSN (Online) : 2230-8849
Volume 5 Issue 2 July - December 2015
International Manuscript ID : 22308849072015-01

REFERENCES

[1] Marco Conti, Body, Personal and Local Ad Hoc Wireless Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 1), CRC Press LLC, 2003.

[2] M. Weiser, The Computer for the Twenty-First Century, Scientific American, September 1991.

[3] M.S. Corson, J.P. Maker, and J.H. Cernicione, Internet-based Mobile Ad Hoc Networking, IEEE Internet Computing, pages 63–70, July-August 1999.

[4] Amitabh Mishra and Ketan M. Nadkarni, Security in Wireless Ad Hoc Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, 2003.

[5] Lidong Zhou and Zygmunt J. Hass, Securing Ad Hoc Networks, IEEE Networks Special Issue on Network Security, November/December 1999.

[6] Yongguang Zhang and Wenke Lee, Security in Mobile Ad-Hoc Networks, in Book Ad Hoc Networks Technologies and Protocols (Chapter 9), Springer, 2005.

[7] Panagiotis Papadimitraos and Zygmunt J. Hass, Securing Mobile Ad Hoc Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 31), CRC Press LLC, 2003.

[8] Yi-an Huang and Wenke Lee, A Cooperative Intrusion Detection System for Ad Hoc Networks, in Proceedings of the 1st ACM Workshop on Security of Ad hoc and Sensor Networks, Fairfax, Virginia, 2003, pp. 135 – 147.

[9] Data Integrity, from Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Data_integrity.