Fostering a Secure Framework for National Research and Education Network

By

Ajayi Olutayo B. and Ajayi Ibironke A.

Introduction

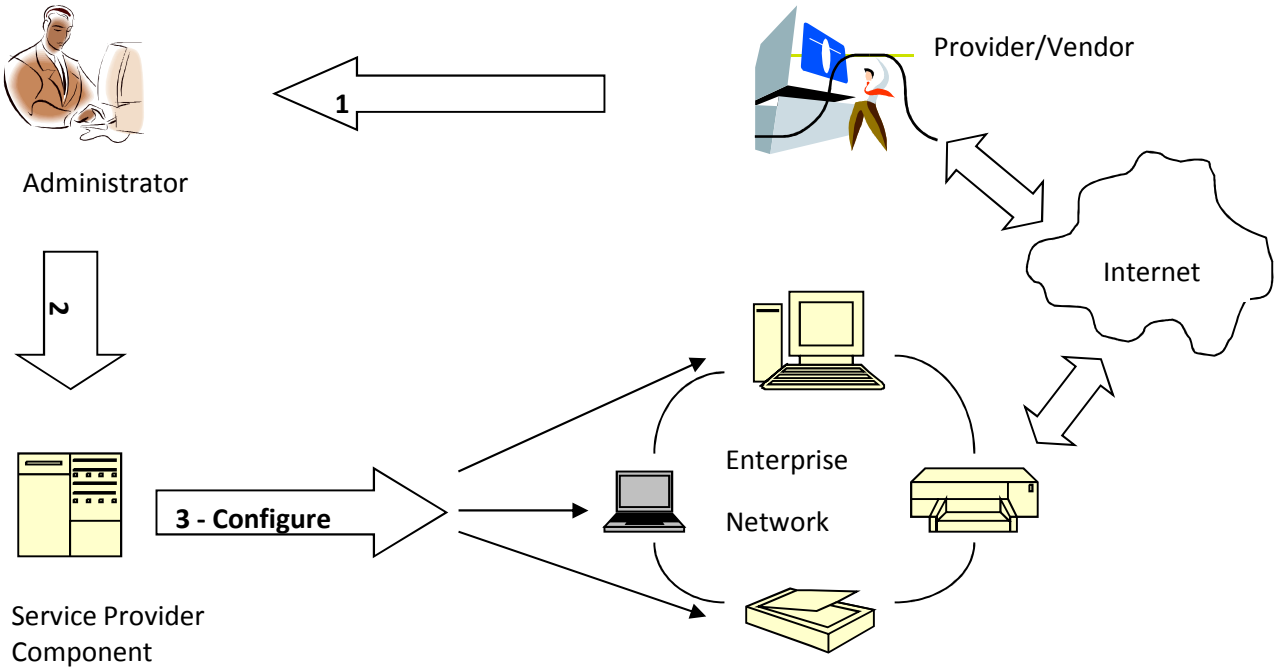
- This paper examines the security concerns and novel secured framework on deployment of National Research and Education Network (NREN) that is not exploited by malicious interference of shared resources.
- A Research and Education Network (REN) is an association of institutions that is focused on conducting research and educational instructions, with the aim of institutional collaboration for the purpose of maximising scarce resources, proffering solutions and improving infrastructure for the realisation of their organisational objectives
- The need for interconnectivity and interoperability does not imply that security issues should be compromised.

Introduction (cont..)

- Different user communities require different levels of security. Each network on which the national information infrastructure is built must have a number of security procedures implemented that will prevent unauthorized access to the network and the systems that comprise it.
- Network technologies and services are now regarded as essential to support distributed research communities around the world. The development of these services however is in its infancy and the services will continue to evolve over the years in Africa.
- Emphasis should be geared towards using frameworks that are developed on minimal hardware pushing some of the resources to be managed by fewer secure managed devices.

Introduction (cont..)

- A typical Network Service Configuration Scenario



The Approach

- The current trend is to deploy mobile agents to manage such large heterogeneous networks like NREN. Mobile agents are special software objects that have the unique ability to transport itself from one system in a network to another in the same network.
- The approach is to automate the resource sharing and collaboration using secure mobile-agent resource transfer (SMART) protocol architecture for NREN simply called SMARTREN.
- The paper explores the fostering of a security framework in NREN most especially situated in Africa. The novel method is to explore the use of proposed mobile agent protocol to create a robust NREN services.

Background Concepts

- Mobile Agents (MA) are intelligent autonomous programs that can travel across the heterogeneous network in order to perform an assigned task.
- Mobile Agents are one of the popular and simpler ways of retrieving information from the Internet.
- Aglets are fundamentally Java-based autonomous software mobile agents. An aglet carries its state and as well as data along with it while traveling across the network.
- Basic idea: Create once, go anywhere.

Background Concepts (cont..)

Significance of Mobile Agent

- Reduces Network Traffic.
- High Scalability.
- Asynchronous processing.
- Support for heterogeneous environments.

Background Concepts (cont..)

- The multi-signcryption protocol is a cryptographic method that fulfills both the functions of secure encryption and digital multi-signature for multi-users, at a cost smaller than that required by multi-signature-then-encryption (Mitomi, 2001; Pang, 2003; Seo, 2004).
- In this paper, a Discrete Logarithm (DL) based multi-signcryption protocol to the Elliptic Curve (EC) based multi-signcryption protocol (DL-MEC) was used to design the secure mobile agent resource transfer REN protocol (SMARTREN).
- Multi-signcryption = multi-signature + encryption

Related Works

- It is critical to recognize that even in the present Internet, it has been possible to accommodate a remarkable amalgam of private enterprise, academic institutions, government and military facilities.
- The Internet services do serve the public but extremely vulnerable to mass attacks, although the linkages between the Internet and the public make the system extremely accessible to a very wide variety of users.
- Some NRENs in Africa that are presently sharing contents between members and provide their clients with research networks and Internet without necessarily providing a robust and secured networks using minimal hardware solutions.
- The needs and benefits of these technologies do not imply that security issues should be compromised.

Model and Design

- Design Requirements:
- The concern is the practicalities of securing the agent using a very useful and simple approach to devise signed itinerary. Supplied with signature verifiable itinerary an agent has the knowledge about where to go and what to do before it embarks on its journey. In addition to these basic requirements, the agent dictates an alternative set of actions should some foreseen or unforeseen event occur. Agent travels the network following some predetermined itinerary, upon completion of the task the agent will send feedback.

System Model and Design

- SMARTREN station assumes responsibilities of a client. All managed nodes are servers, which has mobile agent execution environment and respond to SNMP queries from mobile agents when they visit the servers and manipulate data locally. When the client in the SMARTREN needs access to data in a network-connected device, it does not talk directly to the server over the network but dispatches a mobile agent to the server's machine. On arriving at the servers' machine, the mobile agent makes its request and return to the management station with the results.

System Model and Design (cont..)

- The SMARTREN architecture consists of the following major components:
  - Management application (MA)
  - Mobile Agent Execution Environment (MAEE)
  - Secure Mobile Agent Producer (SMAP)
  - Mobile Agents (MA)
  - Modified Multi-signcryption protocol (MMSP)
- In the SMARTREN architecture, the mobile agents are provided with:
  - The list of nodes to be managed
  - SNMP statistics of interest
  - Health functions as defined by the user
- Development environment is the Aglet Software Developer Kit (ASDK)

System Model and Design (cont..)

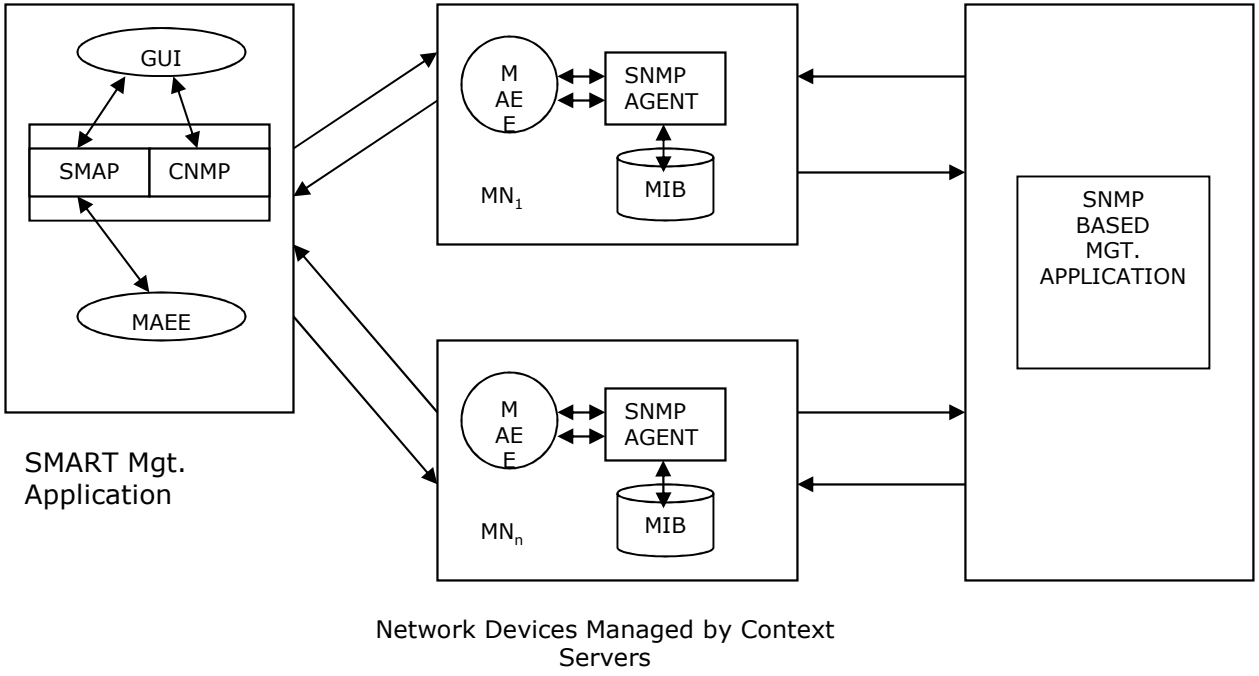


Figure 1: Hybrid SMARTREN Model

System Model and Design (cont..)

Basic Solution

- The idea is to use the basic solution to evaluate the proposed secure protocol. Elliptic Curve based Digital Standard Signature scheme (Menezes, 1997) was appended to the existing SNMP nodes for user authentication and integrity of data. It was assumed that the existing nodes already establishes a common secret key K_i between ith Managed Node and the SNMP based Context Servers (CS) of the Management Centre (MC), and provides confidentiality through a private key cipher algorithm with Ki.

System Model and Design (cont..)

- The basic solution is as follows:

[**EC-DSS Generation and Encryption phase**]

- MN_i generates a signature on the itinerary data M_i as follows:
  - MN_i chooses random k_i R [1, ..., q − 1], and computes $r_i = k_iG \pmod q$
  - MN_i computes $s_i = (H(M_i) + r_ix_i) \cdot k_i^{-1} \pmod q$
- MN_i encrypts M_i with K_i, i.e., it generates $C_i = ENC_{Ki}(M_i)$.
- MN_i sends (r_i, s_i, C_i, ID_i) to the MC.

[**EC-DSS Verification and Decryption phase**]

- After the MC receives (r_1, s_1, C_1, ID_1), (r_2, s_2, C_2, ID_2), ...,(r_n, s_n, C_n, ID_n) from network gateways, it decrypts the C_i and obtains the itinerary data M_i of MN_i.
- MC verifies the signature (r_i, s_i) of MN_i as follows:

  (a) MC computes $r_i' = (H(M_i)G + r_iY_i) \cdot s_i^{-1} \pmod q$.

  (b) MC checks $r_i = r_i'$.

System Model and Design (cont..)

SMARTREN Protocol Using EC Multi-signcryption

- The work presented a secure mobile agent protocol for network management services in network environments. The protocol consists of four procedures such as:
  - Certification procedure
  - Mobile agent creation procedure
  - Mobile agent execution procedure
  - Mobile agent arrival procedure
- It provides confidentiality and integrity for the itinerary data, and user authentication using EC Multi-Signcryption. An overview of the proposed security model of the SMARTREN protocol is shown below.

System Model and Design (cont..)

- **Preparation and creation procedure**

In this procedure, the SMARTREN calls a mobile agent MA and determines the migration path of MA, $MA_{route} = MN_1||MN_2||...||MN_n$. Then it creates itinerary request message itireq, and generates a signature on itireq as follows:

- SMARTREN chooses random number k_C R [1, ..., q − 1] and computes $R_C = k_C G$.
- SMARTREN computes $r_C = H(itireq||ID_C||R_C)$ (mod q) and $s_C = (x_C + r_C) \cdot k_{-1}{}^C$ (mod q).
- SMARTREN gives itireq, MA_{route}, and signature, (ID_C, r_C, s_C) to the MA, and the MA migrates to the first manager's network gateway, MN_1 with them.

System Model and Design (cont..)

- **Execution procedure**
- After the MA has migrated to $MN_i (1 \leq i \leq n)$, MN_i checks the itireq and MA_{route}.
- MN_i verifies the SMARTREN's signature and generates the EC Multi-Signcryption on its itinerary data, M_i
- **Arrival Procedure**
- After the MA finishes the travels of the migration path MA_{route}, it arrives at the SMARTREN.
- MA gives (ID_1, s_1, C_1), ..., $(ID_{n-1}, s_{n-1}, C_{n-1})$, and (ID_n, r_n, s_n, C_n) to the SMARTREN.
- SMARTREN performs the EC Multi-UnSigncryption to verify and decrypt the EC Multi-Signcryption message.

System Model and Design (cont..)

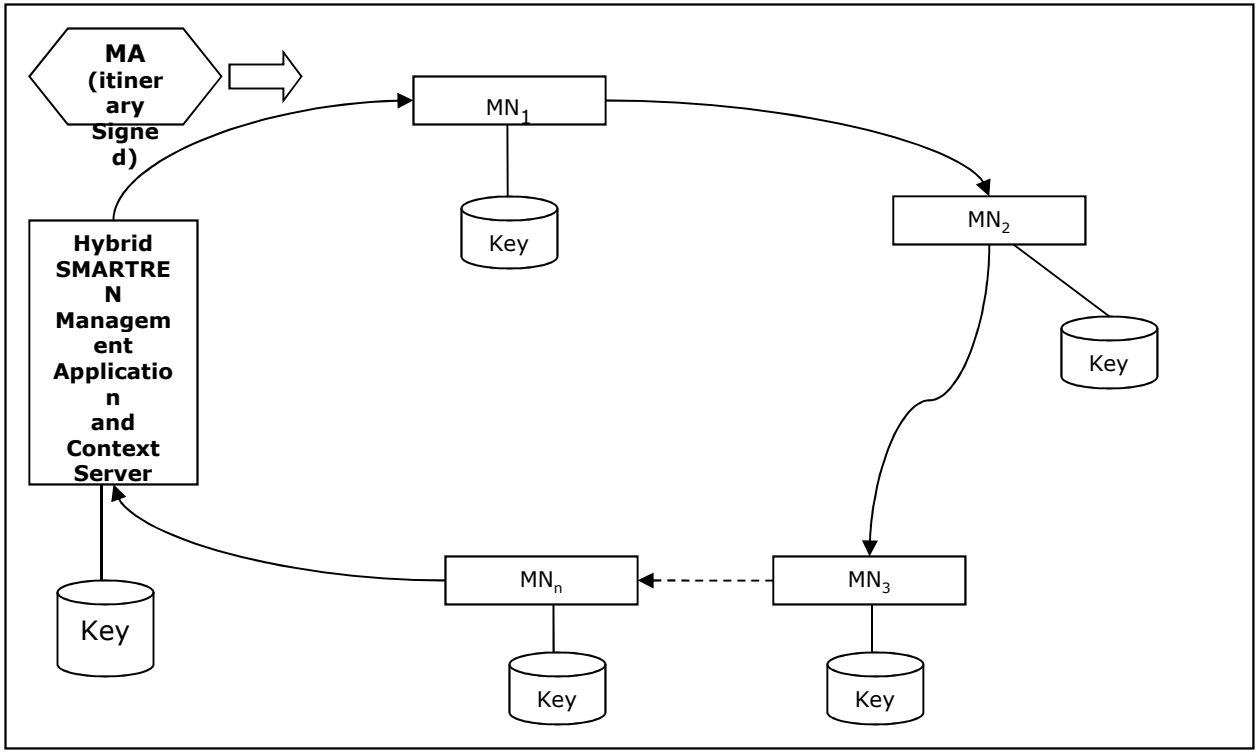


Figure 2: Security Model for SMARTREN Protocol

System Model and Design (cont..)

The sequence of events on the security model is as follows:

1. The management application decides to send MA to a set of network devices
2. It constructs an itinerary for the MA and digitally signs it with private key that it keeps in keystore. Thereafter, starts its journey to its first destination.
3. The MA bytecode is authenticated using appropriate policy by verifying the signature of its itinerary using the key in the keystore.
4. Once the itinerary is verified, the MA begins its job by performing the management tasks assigned to it through querying the SNMP agent. Then MA constructs its information objects to be handed over to management application when it will return.

System Model and Design (cont..)

5. The MA generates a key and encrypts the information object with it using the MMSP public key of the MA.
6. The MA then dispatch to the next destination with its encrypted objects.
7. The MA repeat the sequence in steps 3 to 6 until the last destination with all accumulated encrypted session keys and information objects.
8. The MA then dispatch itself back to SMARTREN station where all objects is handed over and thereafter terminates itself.
9. The SMARTREN station decrypts the session keys using the private key and also using the session keys to decrypt the information objects.

It prevents eavesdropping and tampering since the MA itself has no access to its private key which is stored in SMARTREN key database.

Implementation and Evaluation

- For the performance indicators of SMARTREN and to interact with the SNMP agent, the work employed the use of AdventNet SNMP to get parameters needed for the work. This simulation package provides a set of java tools for creating cross platforms Java and Web-based SNMP network management applications.
- Also to study the behaviour of SMARTREN in carrying out network management tasks, we used Network Simulator (NSMAN) referred to as NS-2, a discrete event simulator targeting at network research.
- Also, the use of SNMP table filtering and limited fault tolerance features were added to the SMARTREN architecture described in the subsequent section.

Implementation and Evaluation

The primary measure used for network utilization is interface utilization (used in NS-2 simulation). The formulas are:

For half duplex:

$$U(t) = \frac{(ifInOctets + ifOutOctets)*8*100}{ifSpeed * SysUpTime}$$

For full duplex:

$$U(t) = \frac{max(ifInOctets, ifOutOctets)*8*100}{ifSpeed * SysUpTime}$$

Implementation and Evaluation

- Table Filtering Capabilities:
- SMARTREN have the potential to improve the retrieval of SNMP tables in terms of network overhead. Using the successive GET-NEXT request, SMARTREN gets the filtered snapshot of the table, encrypts it and saves it. Once the SMARTREN has the SNMP table it can flexibly filters the values according to a filter saved in it. The filtering expression is defined by user. The work is to fetch the ifTable and filter according to column ifInError(ifInError.value >7).

Implementation and Evaluation

- With the performance indicator analysis, the SMARTREN architecture can provide an extremely powerful, flexible and adaptive environment for the purpose of assisting network management. This proves advantageous over existing client/server architecture in the following areas:
  - Message Confidentiality
  - Message Integrity
  - User Authentication
  - Non-repudiation
  - Robustness
- The protocol was evaluated from a point of view of communication overhead, response time and compare the protocol with the basic solution as shown below.

Implementation and Evaluation

- **Message Confidentiality**: The attacker cannot know SMARTREN's private key, x_C, he cannot compute session keys due to the difficulty of the elliptic curve discrete logarithm problem
- **Message Integrity**: SMARTREN can verify forged signature in the EC Multi-UnSigncryption phase.
- **User Authentication**: SMARTREN can confirm the identity of the Administrator, U_i, through the ID_i included in the EC Multi-Signcryption message.
- Since MN_i of U_i generates the EC Multi-Signcryption, he cannot falsely deny later the fact that he generated it.
- **Robustness**: If verification fails, it cannot decrypt the cipher text C_i which prevents damage by malicious code in the MA. Therefore, our protocol provides robustness.

Implementation and Evaluation

Fault-tolerance Features

The SMARTREN architecture has also been designed to provide limited fault tolerance features. SMARTREN should be able to survive network and systems failures to secure MA migrations using the scenario below.

- **Step 1**: In the case, the TCP connection establishment fails.
- **Step 2**: The MA records the unreachable host's name into the MA's 'problem folder' and retrieves the next destination host from the itinerary folder.
- **Step 3**: The MA will then migrate to this host. When returning to the manager host, the MA reports the failed devices to the manager application, which in turn will take any necessary fault recovery actions.

Implementation and Evaluation

- The response time of SMARTREN is measured as the mean time of the MA launching time and returning time. The centralized SNMP approach is measured as the mean time of the first GET message was sent out and the last result fetched back (table 1).
- Regarding the health function computation, the SMARTREN info retrieval agent transfer less number of messages comparing to the SNMP method as shown in the table 2 below. Thus, the total message size is reduced and the bandwidth is saved.

Implementation and Evaluation

Table 1: Response Time

	Centralized SNMP Approach	**SMARTREN**
1 host	0.69 Seconds	0.71 Seconds
2 hosts	0.9 Seconds	0.95 Seconds
4 hosts	1.2 Seconds	1.24 Seconds
30 hosts	4.9 Seconds	4.89 Seconds

Table 2: Communication Overhead

	SNMP		**SMARTRENInfoRetrieval Agent**	
	No. of Messages	**Total Message Size**	**No. of Messages**	**Total Message Size**
Interface utilization	4	364Byte	1	35Byte
Interface Accuracy	3	275Byte	1	34Byte
IP Discard Rate	5	458Byte	1	37Byte

Implementation and Evaluation

- SMARTREN has been evaluated in simulated large-scale network environments, using the network simulator (NS-2) tool.
- The application scenario involves polling managed elements for the contents of tcpConnTable MIB-II table, which lists information about all TCP connections of a host. In the SNMP-based implementation, individual MIB tables are remotely retrieved through exchanging request/response messages, in particular by issuing successive get-next requests (each retrieving a table row).

Implementation and Evaluation

- A careful simulation parameters are as follows:

Grouping	Parameter	Value
MA Information	MA initial size State size increment	1.08 kb 98 bytes
Request Information	SNMP packet increment Packet size	17 bytes 90 bytes
Response Information	SNMP retrieval SMARTREN retrieval Packet size	102.1 ms 71 ms 90 bytes
Session Information	Topology Nodes Interconnected links Links with stub Time (ms) Background Utilization (%)	Transit-stub 272 2 mbps 100 mbps 100 25

Implementation and Evaluation

- The sequence of events are as follows:
  - Use of Object Oriented Scripting Language (OTcl) scripts describing the topology using the network component object libraries (nodes, agents etc..)
  - In the OTcl, use event scheduler for traffic sources in transmitting packets
  - SMARTREN agent object class module added and compiled together
  - The Tcl simulation script executed by running the script with NS-2
  - The Network Animator (NAM) tool was used to visualize the behaviour using Xgraph and TraceGraph.

SMARTREN Advantages

- The repetitive request/response handshake is eliminated
- Reduces design risk by allowing decisions about the location of the code pushed towards the end of the development effort
- Resolves problems created by intermitted or unreliable network connections
- Real time notifications
- Parallel executions (or load balancing) where large computations are divided amongst processing resources.
- Offers an alternative to or complementing SNMPv3 security in network management system
- Use of Filtering BULK-request to reduce network load.

The Security Advantages

- Practical scheme for message recovery signature, a novel feature of robustness (a message can not be recovered if the signature verification fails)
- The use of message flexibility (generate signature on a modified message)
- Trails of MA records into the MA's "problem folder" and can be retrieved for audit trail.

Contributions to Knowledge

- This work presented a novel method of secure mobile agent based network management system. Contributions of this work include:
  - The SMARTREN can be used as excellent guidelines for users to design new protocol
  - A highly flexible and adaptive framework where new agents can be written to inhabit the design with little effort
  - The SMARTREN is small and modest as against weightier Artificial Intelligence (AI) and other similar technologies
  - As the design is been understudied, standards will emerge and serious security concerns are overcome that will make SMARTREN use a viable proposition.

Future Work

Other areas will be to address the following issues:

- Testing and practical evaluation of SMARTREN in real-world monitoring applications by research engineers in order to improve the SMARTREN performance;
- Extension of the SMARTREN manager platform with the implementation of a web interface that will allow human administrators to view updated management statistics through a typical web browser and remotely control their network;
- Implementation of a light manager application that will be hosted to resource-constrained mobile devices; the manager will interact with managed devices through a wireless application protocol (WAP).

Conclusion

- This work has presented a framework to design a hybrid model based on secure mobile agent protocol and SNMP strategies. The work gives network administrators flexibility of using any of the two approaches to exploit mobile agent technology in resource transfer. The results show that as the managed nodes increases, the proposed techniques perform better than centralized approach (basic solution). On this note, this work has demonstrated that it is possible to develop a secure mobile agent network management system using Java components and cryptography. To this end, the work has presented reasonable detail on design and experimental level view.

Thank You