Proceedings of the International Conference on
Information Technologies (InfoTech-2017)
20-21 September 2017, Bulgaria

AN AUTHENTICATION MECHANISM TO MANAGE MOBILE AGENTS ALONG WITH SENSOR NODES TO IMPROVE WIRELESS SENSOR NETWORK SECURITY

Nafees Ayub, Zubair Nabi, Naima Sabir

Government College University, Faisalabad
nafees.ayub@gcuf.edu.pk, zubair.nabi@gcuf.edu.pk, naimazubair33@gmail.com
Pakistan

Abstract: The use of mobile agents in sensing networks, while bringing many useful benefits, brings additional security threats to sensor networks too. To deal with this strong authentication methods are required for the authentication of mobile agents in sensor nodes networks. In this Article, a scheme that can authenticate both sensor nodes and mobile agents efficiently without putting much pressure on resources is presented. Performance and security analysis has been done on the given scheme. With little overhead in terms of memory, computation and communications, the proposed scheme is able to authenticate mobile agent along with sensor nodes. The overhead would be much greater if a separate authentication scheme better flexibility against selective node capture attacks from the basic scheme. In term of mobile agents, the proposed scheme provides high resilience against masquerading and unauthorized access attacks.

Key words. Wireless Sensor Networks; Network Security; Network Performance; Mobile Agents; Sensor Nodes.

1. INTRODUCTION

Wireless Sensing Network based on wireless special independent devices with the use of detectors to look after the environmental Changing's i.e. .Temperature of surrounding areas, Sounds of nature, variation in magnitude or position around a central point (Detector/Sensing Device), Pressure and sensation of Air, movement of natural items and Pollution in surrounding areas". The devices which are used in (Wireless Sensor) WS Network are also known as sensing nodes. Whole WS Network Consist on No's of detection stations / small sensing nodes which is portable and tiny weight, who sense and also control the environment, enabling the interaction between Sensor Node and surrounding environment [1].

The Performance of a single sensing node is very short as compare to ability of combined Sensing nodes in Network for large atmosphere. All sensing nodes work in Sensing Network together for excellent and more reliable result. Each node performs as per guideline / Programming instructions.

Wireless Sensing Network is based on four parts (Fig.1):

Sensor's Field: Based on sensor nodes for sense an environment.
Proceeding: Performs the local computation on sensed material.
Communication: Responsible for receiving / sending information between Nodes.
Network: Responsible for Routing Map from Sensing field to Environmental field.

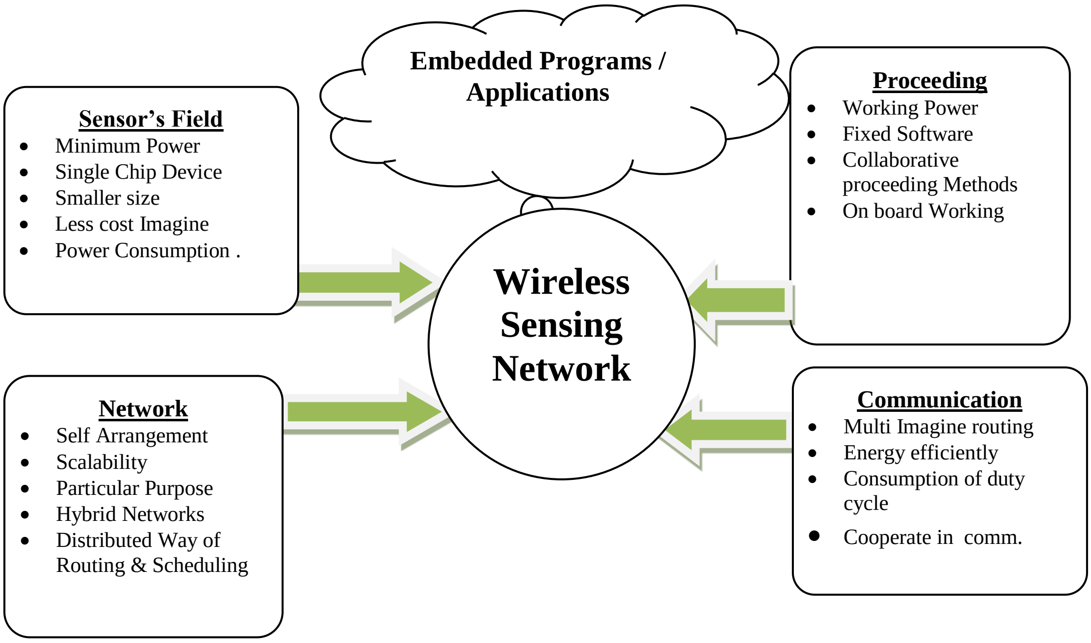

Fig. 1. Explaining Wireless Sensor Networks.

A wireless Sensing network containing large number of detectors nodes. Thickly width in an Area, which is also familiar as the sensing field. The nodes collect information and convert it into signals, a relatively strength node is also called sink node. Sink node basically used forgather data in a WS network from other nodes. For this mechanism a sensor node send data to the nearest sink node. Sink Node is communicated with field of Sensor's does vide wired or Wireless connection and also the sink node performs a gateway role between the sensing network and sensing field. So, quite possible many No's of sink node in a whole Wireless Sensing Network that's depending on the requirement of network [3].Sensor network are used in physical and environmental issues i.e. predictive maintenance, health care, home automation, Improving Productivity, infrastructure monitoring, stock keeping, Enhance Safety &security, energy savings, smart grid computing, traffic control, precision agriculture, urban terrain, mapping and vast range of other applications [6].

1.1. Role of mobile agents in wireless sensing networks

Mobile Agent (MA) is a programmable node as per requirement of the user. Once it is lunched it can move throughout network from one node to another node to perform multiple tasks in different modes. Mobile agents also reduce the wastage of energy and filter the other different agent's unnecessary material and provide exact required data [4].

Major goal of Mobile agent is to Safe the consumption of bandwidth, and shift exact result or required information instead of transfer all raw materials over the network, for this purpose we used special type of agents for filter it. Secondly, the Mobile Agent (MA) have in particular capability to working on Numbers of hosts, dynamically adoption, and mobile User's, software distribution as per requirements, logically routing and easy to maintain [7].

Mobile Agents provide flexibility to re-tasking as compare to other agent in a network. But the requirement of re-tasking may emerge to minor changes to a sensing network to perform tasks that it was not functioning to carry out at first. The requirement of re-tasking may also emerge to perform updates on the Mobile Agents nodes [15].

Mobile agents also provide the facility to process on multiple applications on the whole Wireless Sensing Network. Therefore Mobile agent helps the Wireless Sensor to addition in functionality, Updating and re-tasking existing Program [10, 13].

1.2. Secure issues of sensing networks

Sensing Network tolerate different type of security issues like all other networks. Wireless Sensing Networks needs some Special security Strategy. Due to the incorporation of Mobile Agent in wireless sensing network the network tolerate more security threats.

Normally three types of security threats from MA in wireless sensing network are found, Disclose of material, Refusal of services and Defect of Data. An agent system, made two vital portions: the component and the component platform which can be implement to tolerate security threats from mobile agents. An element is be composed of code and instructed to go through for performance of calculations [2]. The component platform allows the calculating surroundings areas. In sensing networks, the sensing node is work as the agent platform

2. MATERIALS AND METHOD

The developed scheme modifiers the basic scheme in such a way that it is able to authenticate both sensor nodes and mobile agents. While the authentication of sensor nodes is done as in the basic scheme, a few changes are made to accommodate mobile agents. The key pre distribution phase is modified such that the key server can assign keys and IDs to mobile agents too. The phases of the developed scheme are as follows:

2.1. Key pre distribution phase

The key pre distribution phase in the developed scheme is also performed by the key setup server in offline before the deployment of nodes and mobile agents. It consists of the following steps:

For each sensor node s that is to be deployed in the network, the key setup server assigns a unique identifiers IDs.

- For each mobile agent n that is to be deployed in the network, the key setup server assigns a unique identifiers IDm.
- The Key server generates a big key pool **K** of size **N** which consists of randomly generated numbers called symmetric keys.
- The key setup server generates a relatively smaller pool **K** of size **N** which also consists of randomly generated number called symmetric keys.
- For each sensor node s, a random subset Ks of size **n** from the key pool K and K's of size **n** from the key pool K' is selected. K's are then loaded in its memory

Creating a separately key pool for mobile agents gives us some oblivious advantages. A sensor network may consist of thousands of sensor nodes. One mobile agent can cover multiple sensor nodes. The key pool required for authentication of thousands of nodes will be a very large one. Subsequently the subset Ks to be loaded in each sensor node memory will be quite large to ensure proper connectivity between nodes. Therefore if we use the same key pool for both sensor and mobile agents, we will have to load a largest set of keys to each mobile agent's memory to ensure proper connectivity between mobile agents and sensor nodes. This will increase the size of mobile agents which will in turn increase the memory required to store them, the communication cost to transmit them over the network and the computational cost for finding a shared secret key.

Thus using a separate smaller key pool for mobile agents reduce the communicational and computational cost on cost memory required to store a separate subset of keys for mobile agents in each nodes memory. The use of a separate key pool for mobile agents is also strength the security of sensor networks as mobile agents is not be compromised in case a sensor nodes has been captured and its key been decrypted. In case the network in use is small or the number of mobile agents being used in the sensor network is significant (near to the number of sensor nodes in the networks or even greater) then we can use the same key pool for both sensor nodes and mobile agents. Although doing so will increase the chance of mobile agents being compromised in case sensor nodes are captured and their keys are decrypted.

At the time of deployment, each sensor nodes contains its identifiers and two sets of symmetric keys assigned to it. Whereas the time of deployment, each mobile agent contains its identifier and a set of symmetric keys assigned to it.

2.2. Direct key establishment phase

After deployment, the direct key establishment phase for sensor nodes will be exactly the same as in the basic scheme. It has been explained briefly in the basic scheme. That leaving us with mobile agents will be performed only when a mobile agent moves from one sensor node to another. Assume that m is a mobile agent and s is a sensor node. Mobile agent m broadcast its ID to sensor node s and vice versa. After receiving the IDs of each other, both m and s calculate the key IDs of the keys residing in their key rings. For this purposed they use a secret one way function which takes as its inputs their IDs and a key and produces a unique identifier for that key. This secret function is programmed into every sensing node's and mobile agent's memory. Any Pseudo random function that can produce a uniform output for a given range can be used here.

The key **IDs** are calculated as follows:

At Mobile Agent n:
For all keys in the key ring of m:
Generate key **ID = PRF Key (IDn ‖ IDs)**
Add keyID corresponding to the key in its key ring.
At sensor Node s:
For all keys in the key ring of **s**:
Generate key **ID = PRF Key (IDs ‖ IDn)**
Add **key**$_{\mathbf{ID}}$ corresponding to the key in its key ring**.**

It is important to note that the key ring being used here come from the smaller key pool generated specifically for the purpose of mobile agent authentication. As discussed in the key pre distribution phase, if the mobile agents and the sensor nodes are using a single key pool, the same key ring will be used for both mobile agents and sensor nodes.

In order to establish secret key between them, the mobile agents *m* and sensor node *s* now only need to exchange the key IDs just generated by them. If there is a common key ID, then corresponding key is taken as the secret key between them. This key is used to secure future communication. The key IDs are deleted from the mobile agent's and sensor node's key ring as soon as the secret key is established to thwart node capture attack.

After key discovery, the secret key between the mobile agent m and the sensor node s is generated as follows:

$$\mathbf{Kns = H\,(IDn \parallel IDs \parallel K1 \parallel K2 \parallel \ldots\ldots\ldots\ldots\ldots \parallel Ks)}$$

Where K1, K2, K3, …, Ks, are the s common keys between the mobile agent m and the sensor node s, H is a secure way hash function and ‖ is the concatenation operator.

The following important properties that hold for sensing nodes are also ensured for mobile agents during this process:

- If a key is same between the mobile agent and sensor node's key rings then the corresponding key ID generated by them would also be same.
- The key ID for the same key are different for each mobile agent and sensor node pair in the network.
- A relationship is defined between IDs of sensor nodes and mobile agents and the key IDs generated by them. A relationship is also defined between the IDs of sensor nodes and mobile agents and the secret key shared by them.

Since the authentication mechanism being used is same for both sensor nodes and mobile agents, the communication steps involved in the process are also almost the same. The communication process for authentication of mobile agents involves the following steps:

1. m sends a message to s inquiring about previous execution of that particular mobile agent.
2. s response to the inquiry with either true or false. In case the response is true, it means that another instance of the same mobile agent has already finished execution on that sensor node .the mobile agent will then query another node. Else if the response is false, it means that the sensor nodes has not yet been covered by any instance of that particular mobile agent. In this case the mobile agent will continue with the authentication process.
3. **n** transmits its own ID to **s**.
4. **s** transmits its own ID to **n**.
5. **n** generate a random nonce **RNn** and sends this nonce a list of already generated key IDs, its own ID and the ID of s to node **s**.
6. **s** also generates a random nonce **RNs** and sends the nonce, alist or already generates key IDs, it own ID and the ID of **n** to mobile agent **n**.
7. After exchanging the key IDs, m computers the secret key **Kns** shared with s, m then sends a message to s which consists of its own ID, the ID of s, a random nonce and a message authentication code (MAC) of these fields under computed key **Kns.**
8. **s** also computes the secret key kms shared with **n**. it then sends a message to **n** which consists of its own ID, the ID of **n** , a message authentication code (MAC) of these fields under computed key **Kns.**

After receiving the last message, both m and s performs MAC verification for that message. If the verification is successful, mobile agents **n** and sensor node s store key **Kns** for further communication.

Agents to agent authentication can be done in much the same manner with a few modifications. But since agent authentication is out of the scope of this thesis, we leave for further consideration. The fire is modeled by agents which gradually spread through the network. Nodes by inserting engulfing fire tuple spaces. Fire includes modeled along the factors which step by step of flowing through the network, the absorption of nodes by setting fire tuples in their local tuples spaces. Fire has long shaped the factors that go step by step around the entire network, absorbing nodes by setting fire to their places of tuples in tuple general. Factors fire trackers have gone applied to build a fire about border.

2.3. Path key establishment Phase

The path key establishment phase if required will be performed exactly as it is in the basic scheme. Furthermore, the path key establishment phase will only be performed for sensor nodes. Path key establishment is not necessary for mobile agents because even if a mobile agent fails to establish a shared key with a sensor node during the direct key establishment phases, it will just skip the sensor node. That sensor node will be covered by another instance of that particular mobile agent.

3. RESULTS

Security threats in wireless sensing network due to the adding of mobile agents is categorized in four main categories: an node attacks on platform of agents and an agent attacks on other agent at same platform that's the scope of this research work and other's two categories are: an platform of agents attack on agent and other thing attacks the agent Platform [5].

The scope of study on first two categories of attacks (Node attack on platform of agents and an agent attacks on other agent at same platform) – fig. 2. And also study on the main protection and security from these attacks on each Sensor Node and also on Sensor platform.

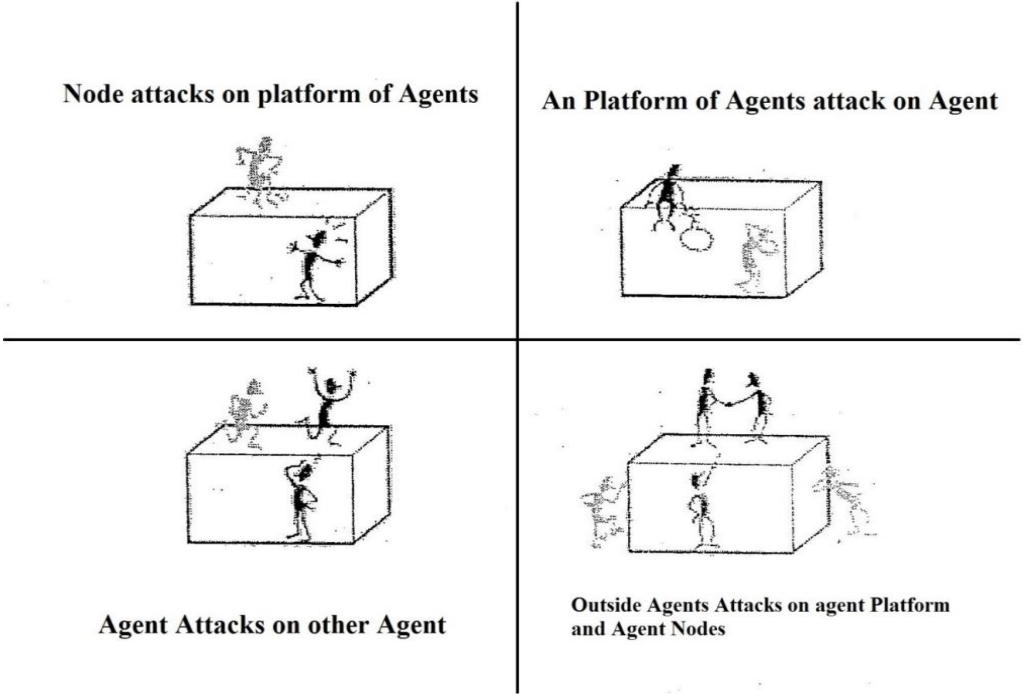
Node attacks on platform of Agents
An Platform of Agents attack on Agent
Agent Attacks on other Agent
Outside Agents Attacks on agent Platform and Agent Nodes

Fig. 2. Agent and Nodes Behaviour

We found out that key arrangement did not execute among two neighbour nodes that contributed less then s keys, where s ≥ 1. Therefore, for the network to be connected, each node must be share at least 1 key with its neighbour [8].

Let $P_{connect}$ denote the possibility that two neighbour nodes shared adequate keys to form a safe link. If N was the key pool side and n was the key ring size, then $P_{connect}$ =1- (Possibility that two nodes contributed to sufficient keys to form a link)

From the basic scheme we knew that $P_{connect}$ =1- [(N-n)/n] / (N/n)

$$= \prod_{i=0}^{n-1} \frac{N-n-i}{N-i}, \text{if } s = 1 = 1 - \sum_{i=0}^{s-1} pi, \text{if} \geq 2$$

Where Pi is the possibility that two nodes have approximately "I" keys common in their key rings and Pi= [(N/n) (n/i) {(N-n) / (n-i)}] / $(N/n)^2$

In proposed scheme, we try to devise a method that supports dual authentication (that can authenticate both sensor nodes and noble agents). We take the identity based random key pre distribution scheme presented by Das (2008) and modify it such that it can authenticate mobile agents along with sensor nodes – table 1.

Table 1. Comparison of performance of existing WSN and MA Authentication schemes [9]

Scheme	Identity Based Random Key Pre Distribution	Proposed Scheme	Digital Signatures	Execution Tracing
Authentication	Sensor Nodes	Both	Both	Mobile Agent
Requirements	Random Key Pre Distribution	Random key Pre Distribution	PKI/TTP	None
Computational Cost	Low	Low	Very High	High
Communication Cost	Low	Low	Low	Low
Memory Cost	Increases with Network Size	Increase with Network Size	Comparatively High	High
Feasible for WSN	Yes	Yes	No	No

4. DISCUSSION

4.1. Security analysis

The protection investigation of the proposed scheme under the random node capture attack, the selective node capture attack and node fabrication attack would be the same as that of the basic schema. The security analysis for these attacks is discussed in brief below. The security analysis for masquerading and unauthorized access attacks is also discussed. These attacks are brought by mobile agents to sensor network.

4.2. Random node capture

In the basic haphazard key pre allocation schemes, the protection of sensor networks is analysed on the basic of the number of communication relations compromised due to captured sensor nodes. In those schemes the flexibility aligned with node capture is measured on the basis of random capture of nodes. Since proposed scheme is based on the identity based random key pre allocation schema presented by Das, the flexibility aligned with node capture of the proposed schema is the same as that of Das. Thus, is the number of sensor captured is small, proposed scheme provides better flexibility aligned with random node capture than the basic random key pre allocation schemes.

4.3. Elective node capture attack

An attacker can selectively capture important nodes to get valuable information instead of randomly capturing nodes. For example an attacker, after inspecting all the keys captured nodes, find a minimal set of sensor nodes that can cover up the highest number of keys in the key pool. However, since keys are dispersed randomly to sensor nodes, the attacker is unable to gain significant information in the selective node capture attack than the haphazard node capture attack. Therefore, like the basic scheme, discriminating node capture attack is insignificant in proposed scheme too.

4.4. Node communication attack

In this kind of attack, the attacker captures some nodes in the network and then on the basic of information gathered those nodes, fabricated some fake nodes. Like the basic scheme, in proposed scheme too, a fabricated node must satisfy two conditions so as to connect to the network through an uncompromised node. These are:

1. The fabricated node should share at least q number of keys with the uncompromised node.
2. If the initial situation is true, every one of the joint secret pair wise keys must be already identified to the attackers.

To satisfy the first condition, the security of proposed scheme depends on the security of PRF function. In order to share q keys with an uncompromised node, the fabricated node should be capable to compute the IDs of the keys residing in its key ring.

From the (Das 2008), we note that like the basic scheme, proposed scheme significantly improves protection aligned with the node fabrication attack then the existing haphazard key Pre allocation schemes.

4.5. Masquerading

In masquerading attacks, the factor or agent platform assumes the ID of a different factor or agent platform. This is done in order to deceive an agent or an agent platform. In case of sensor networks, the agent platform will be the sensor node itself. Proposed scheme provides strong authentication on the basis of identity and creates a link between the identity of an agent, an agent platform and key IDs calculated by them. There also exists link the IDs of the agent ant the agent platform and the secret key generated by them. Therefore proposed scheme provides high resilience against masquerading attacks.

4.6. Unsanctioned access

In unauthorized access threats, an agent or a process may try access data, services and resources of the agent platform for which it has not been generated permission and privileges. Access control mechanism is implemented to deal with these kind of threats. An agent must be properly authentication before allowing it any access to services and resources of the agent platform and it must be made sure that the agent only has access to the service and resources that it has been authorized for. Since proposed scheme provides strong agent and platform authentication, unauthorized access attacks are less likely (Table 2).

Table 2. Comparison of Security of existing WSN and MA Authentication schemes with proposed scheme [13].

Scheme	**Identity Based Random Key Pre Distribution**	**Proposed Scheme**	**Digital Signatures**	**Execution Tracing**
Resilience against Random Node Capture	Batter Then rest	Batter Then rest	High	-------
Resilience against Fabrication Attack	Insignificant	Insignificant	High	-------
Resilience against Fabrication Attack	High	High	High	-------
Resilience against Masquerading	High	High	High	Low
Resilience against Unauthorized Access.	High	High	High	High

Now suppose a fire breaks out in the forest and the sensor nodes are no required to monitor the fire. In order to do that, mobile agents are deployed into the network to update the nodes for the required task. We assume that mobile agents are split into different categories based on the actions they perform. The mobile agents, in this case, belong to category A of mobile agents and are only responsible for updating the nodes to monitor the fire. Mobile agents belonging to other categories may also be deployed in the network to perform other tasks. In this case study I shall consider only agents belonging to category A.

Now mobile agents A1, upon deployment, will need to authenticate itself with sensor node A, it will send an inquiry message to node A regarding previous execution of a mobile agent from similar category. The node A will response in negative. The mobile agent A1 will then send it ID to node A. node A will its ID to mobile agent A1. Both will calculate the key IDs of the keys residing in their key rings by passing values to the PRF function. The node will use the mobile agent key ring for calculating key IDs. After this both the mobile agentA1 and the node A will broadcast their key IDs to each other. Upon receiving key IDs, common key IDs will be found and the respective keys will be used to generate the secret shared key. A

MAC authentication will then be performed. If the MAC authentication is successful, the key will be used as the secret shared key for future communications. In our case study, upon successful authentication, the mobile agent will just jump to the destination node in order to perform its operation

5. SUMMARY

Security is a main anxiety in sensor network, the lack of security can sometimes undermine the functionality of an entire sensing network. The use of mobile agents in sensing networks, while bringing many useful benefits, brings additional security threats to sensor networks too. To deal with this strong authentication methods are required for the authentication of mobile agents in sensor nodes networks. Currently, no specific method exists that can authenticate both sensor node and mobile agents in sensing networks. While separate solution do exist, the use of separate mechanism for authentication of sensor nodes and mobile agents are not feasible in the resource restrained sensor networks [10, 11].

In this article we presented a scheme that can authenticate both sensor nodes and mobile agents efficiently without putting much pressure on resources. We take the identity based haphazard key pre allocation schema presented by for sensor node authentication and modify it such that proposed schema presented authenticates mobile agents too along with sensor nodes [13]. The scheme has 3 stages. The key pre allocation stage, the direct key establishment stage and the path key organization stage. We modify the key pre allocation stage such that the key setup server assigns IDs and key to mobile agents too. Two approaches are discussed. One is the separate key pool approach and the other is the same key pool approach. In the separate key pools are created for sensor nodes and mobile agents. This approach proves to be costly if the size of the sensor network is small or if the number of mobile agents roaming the network is near or equal to the number of sensor nodes. When this is the case, the single key pool approach can be used.

The direct key establishment phase will be exactly the same as done in the basic scheme by Das. Mobile agents will be authenticated in a similar manner with different parameters. It is important to note that mobile agent’s authentication will only be done when a mobile agent moves from on node to another. The path key establishment will only be performed for sensor nodes. We don’t need path keys for mobile because multiple instance of the same mobile agent roams the network.

In the end, performance and security analysis has been done or the given scheme. Proposed scheme achieves the same network connectivity as that of the basic scheme. With little overhead in terms of memory, computation and communications, proposed scheme is able to authenticate mobile agent along with sensor nodes. The overhead would be much greater if a separate authentication scheme better flexibility against selective node capture attacks from the basic scheme. In term of mobile agents, proposed scheme provides high resilience against masquerading and unauthorized access attacks.

6. CONCLUSION

The case study reveals that with only a slight increase in the computational cost of the basic scheme, proposed scheme is able to authenticate mobile agents along with sensor nodes. Although, the memory and communication overhead is significant, almost equal to that of the basic scheme, it would be far less than the overhead incurred due to the use of a separate scheme for the authentication of mobile agent in sensor networks. Furthermore, proposed scheme utilizes the same setup as that of the basic scheme and no infrastructural changes are required. In case we use of a separate scheme for mobile agent authentication, software and hardware changes will be required to the infrastructure to accommodate the new scheme. These advantages make proposed scheme for more feasible to be used for mobile agent authentication in sensor networks. The need of using a separate scheme for mobile agent authentication is eliminated.

REFRENCES

[1] Akyildiz, I.F., W. Su, and E. Cayirici, 2002 Wireless Sensor Network: a survey, IEEE Communication magazine 40(8):102-114

[2] Alfalayleh, M. and L. Brankovic, 2004. An overview of Security Issues and Techniques in Mobile Agents, the shool of Electrical Engineering and Computer Science, The university of Newcastle, Newcastel, Australia.

[3] Anad M., E Cronin, M sherr, M.A Blaze, Z.G. Lve and I. lee 2006. Sensor Network security, More interesting than you think, Department of Comp. & Info Science, Dept. paper (CIS), Pennsylvania University.

[4] Aouadi, H. and M. B. Ahmad 2006. Security enhancements for Mobile Agents platforms, IJCSNS international journal of Com. Science and network security, 6(7B): 216-221

[5] Ayyaswaproposed K., and S. Rengramanajuam 2010, self-umpiring system for security in wireless Mobile adhoc Network. Wireless Sensor Network, 2(3): 264-226

[6] Bharathidasan, A., and V. A.S Poudurn 2003. Sensor Network: An overview, department of computer science, University of California, Davis, CA 95616.

[7] Borselius, N., 2002 mobile agent security, Electronics & Communication Engineering IEEE, London UK 14(5):211-218.

[8] Camtepe S.A and B Yener 2005. Key Distribution mechanism for wireless sensor network. A survey, Technical Report TR-05-07, Department of computer science, Rensselaer Polytechnic Institute.

[9] Chan H., A. Perrig and D. Song, 2003.Random Key Pre Distribution scheme for sensor network. In IEEE symposium on Security and Privacy, March 2003

[10] Chan M., T Kwon, Y Yuan and V. C.M leung 2006. Mobile agent Based wireless sensor Networks. Acadeproposed Publishers, Journal of computer 1 (1): 14-21.

[11] Culler, D.D estrin and M. srivastava, 2004. Overview of sensor Networks. University of California. IEEE, 37(8): 41-49.

[12] Chong,C and S.P. kumar 2003. Sensor Networks: Evolution, opportunities and challenges, proceedings of the IEEE, 91 (8): 1247-1256

[13] Das, A. K., 2008 An Identity-Based Random Key Pre-Distribution Scheme for Direct Key Establishment to Prevent Attacks in Wireless Sensing Networks, International Journal of Network Security (IJNS), Vol.6, No.2, PP.134–144, Mar. 2008.

[14] Fok, C. G Roman and chen yang Lu, 2005. Mobile agent middleware for sensor networks. An application case study, Washington University in saint Louis, saint Louis, Missouri.