Secured Directed Diffusion using Mobile Agents

Waseem Ahmed
Research Scholar
YMCA University of Science and Technology
Faridabad

Preeti Sethi
Assistant Professor
YMCA University of Science and Technology
Faridabad

Naresh Chauhan
Professor
YMCA University of Science and Technology
Faridabad

ABSTRACT
Wireless Sensor Networks comprise of innumerable small sensors that have limited resources. As wireless sensor networks are usually deployed in remote and unfriendly environment to transmit sensitive and crucial information, sensor nodes are vulnerable to node compromise attacks. Security issues such as data confidentiality and integrity which are of utmost importance need proper consideration in WSN**.** Hence, wireless sensor network protocols, as data aggregation protocol, must be designed keeping secrecy in mind. The work aims to use software agents to introduce security features in an agent based environment which is known as Secured Directed Diffusion using Mobile Agents (SDDMA). It extends the IDDMA approach by adding encryption to it**.** This will help to determine the sequence of target nodes to be visited by the Mobile Agent along with the encrypted data.

Keywords
Mobile Agent Directed Diffusion, Wireless Sensor Networks, Secure Data Aggregation, Cryptography.

1. INTRODUCTION
Wireless Sensor Networks (WSNs) comprise of a number of smart sensors well equipped to sense, process data and communicate to acutely resource constricted devices. The computing model adopted by each sensor node will actually determine the performance of the WSNs. Recent researches more or less focus on routing protocols traditionally based on the client/server (c/s) computing model in [1]. The c/s model is tagged with several problems in WSNs applications that the sensors collect data and deliver them to sink parallel. So the excessive amount of sensory data to be delivered is bound to cause unpunctual delivery, immense energy consumption and load maladjustment among sensors. Owing to a large number of nodes densely distributed in WSN, energy, storage space and the computing capability are generally limited. This makes WSN vulnerable to be invalid and maintenance becomes difficult.

The limitations of C/S computing model applied in WSN account for the necessity of studying and adopting new computing method. The unique capabilities of mobile agent [7] computing model, such as self-governance, intelligence and mobility provides a new model for distributed computation which helps overcome the shortcomings of C/S computing model. In mobile agent computing model, agent entity carries- execution code, running status, process result and it accesses its path by itself and moves independently in the network and interacts with the outside in which self-governance and coordination are emphasized

2. SECURITY ISSUES IN WSN
Due to unfriendly environments and unique capabilities of wireless sensor networks, it is an adventurous task to protect sensitive information transmitted by wireless sensor networks [8]. In addition, wireless sensor networks encounter security problems which traditional networks generally never face. Therefore, security is of prime importance for wireless sensor networks and there are many security considerations that should be looked into. In this section, we present the essential security requirements that are raised in a wireless sensor network environment and have elaborated these requirements related to data aggregation process [8].

2.1 Data Confidentiality
Data confidentiality is probably the most common aspect of information security. In wireless sensor networks, data confidentiality ensures that secrecy of sensed data is never disclosed to unauthorized parties and it is an issue of utmost importance in mission critical applications. It is expected that a sensor node should not pass on its readings to neighboring nodes. Moreover, in many applications, sensor nodes transmit highly sensitive data, e.g., secret keys; In the military, concealment of sensitive information is major concern and therefore it is absolutely important to build secure channels among sensor nodes.

2.2 Data Integrity
Although data confidentiality ensures that only intended parties obtain the un-encrypted plain data, it hardly protects data from being altered. Data integrity guarantees that a message being transferred is never disturbed. A malicious node may corrupt messages to prevent network from functioning properly. In fact, due to untrustworthy communication channels, data may be altered without the presence of an intruder.

2.3 Source Authentication
Since wireless sensor networks work on a common wireless medium, any unauthorized entity can intrude the sensor nodes. So, the sensor nodes need authentication mechanisms to detect maliciously injected or spoofed packets. Source authentication enables a sensor node to ensure the identification of the peer node it is in communication with. Without source authentication, an

opponent could masquerade a node, thus gaining illegal access to resource, crucial information and interfering in the operations of other nodes. Moreover, a compromised node may send data to its data aggregator under several fake identities so that the integrity of the aggregated data is doubtful. Faking multiple sensor node identities is called Sybil attack [5].

2.4 Availability

Availability ensures the workability of network services against Denial-of-Service (DOS) attacks. A DOS attack can be started at any layer of a wireless sensor network and it may disable the victim node(s) permanently. In addition to DOS attacks, increase communication or computation may finish off battery charge of a sensor node. Consequences of availability loss may be drastic.

3. DATA AGGREGATION

Wireless sensor networks generally comprises of a huge number of cost efficient sensor nodes that have constricted sensing, computation and communication capabilities. Due to restriction of sensor nodes resources, minimization of data to be transmitted is preferable as it improves the life of sensor and its overall bandwidth utilization is improved [8]. Data aggregation is the process of accumulating and reorganizing sensor data so as to lower the amount of data transmission in the network.

Data aggregation protocols in wireless sensor network must satisfy the security requirements explained in above section. However, the resource constraints of sensor nodes and necessity of plain data for aggregation process poses great challenge when security and data aggregation together are put to work[8]. Security requirements of wireless sensor networks can be satisfied using either symmetric key or asymmetric key cryptography.

Security and data aggregation are together achieved in a hop-hop fashion. However, data aggregation protocols usually cannot aggregate encrypted data. Therefore, such data aggregation protocols must decrypt the sensor data to perform data aggregation and encrypt the aggregated data before transmitting it**.**

That is, data aggregators must decrypt every message they receive, aggregate the message according to the corresponding aggregation function, and encrypt the aggregation result before forwarding it.

This entire process of data aggregation and providing security is done by the agent in the agent based computing system.

4. RELATED WORK

The task of imbibing mobile agents in the field of wireless sensor networks has been attracting researchers because of unique features described above. This section presents the work of various eminent researchers in this field.

Kemal Akkaya *, Mohamed Younis [3] surveys recent routing protocols for sensor networks and presents a classification for the various approaches pursued. The three main categories explored in this paper are data-centric, hierarchical and location-based.

Chalermek Intanagonwiwat, Ramesh Govindan, Deborah Estrin, John Heidemann, and Fabio Silva [2] explore the *directed diffusion* paradigm. Directed diffusion is data centric in that all communication is for named data. All nodes in a directed diffusion-based network are application-aware. This enables diffusion to achieve energy savings by selecting empirically good paths and by caching and processing data in-network (*e.g.*, data aggregation).

Suat Ozdemir, Yang Xiao [8] proposed that due to restriction of sensor nodes resources, minimization of data to be transmitted is preferable as it improves the life of sensor and its overall bandwidth utilization is improved [8]. Data aggregation is the process of accumulating and reorganizing sensor data so as to lower the amount of data transmission in the network.

As wireless sensor networks are usually deployed in remote and unfriendly environments to transmit sensitive information, sensor nodes are vulnerable to node compromise attacks and security issues as data confidentiality and integrity are extremely important. Hence, wireless sensor network protocols, e.g., data aggregation protocol, must be designed with security in mind [8].

Wang Jietai, Xu Jiadong, Yang Shaojun [7] suggested that computing model of nodes has an important effect on the network performance. The mobile agent computing model for the next generation network has progressively attracted huge attentions. The background of mobile agent applied in the wireless sensor network is analyzed.

Fei Jiang, Haoshan Shi, Zhiyan Xu, Xiangjun Dong [1] proposed a IDDMA mechanism which takes place in three steps. The first phase is known as **Controlled gradients setup phase,** in which a sink node floods its neighbors an interest message to setup initial gradient values of sensors. In the ***Exploratory Data Dissemination Phase*** of IDDMA, two steps are put forth. The first step is known as FED(first exploratory data) in which Source nodes are sending their identity to the sink and in the second step, each source will flood all its neighbors the data for the second time (the EDP is called SED(second exploratory data)), focuses on setting up TargetSrcTable. In the last phase known as **MA action phase**, agent is dispatched by the sink to the target region for processing and aggregating the sensed data**.** But, no security issues occurred during this approach. Since, sensed data should be secured while travelling on a wireless medium, the author does aim to deal with the problem of security in the following section.

5. PROPOSED WORK

The author aims to propose a mechanism for securely sending the data to sink using agents. Since, sensed data should be secured while travelling on a wireless medium; it is suggested by providing security to sensed data using asymmetric key cryptography.

The SDDMA mechanism is divided into three phases: Controlled gradients setup phase, Target region setup phase and Secured MA action phase.

5.1 Controlled Gradients Setup Phase

In the first phase a sink node floods an interest message to its neighbors to setup initial gradient values of sensors.

Taking both optimal path choosing and load balance into consideration.

5.2 Target Region Setup Phase

In the second phase of SDDMA, two steps are put forth. In the first step source node are sending their identity to the sink along with their public keys.

In the second step of Target region setup phase, each source will flood all its neighbor the data for the second time immediately focuses on setting up *TargetSrcTable*.

5.3 Secured MA Action Phase

In the third phase, a MA will be created by sink and dispatched to the target region to visit the source nodes. When the task is finished, the MA will return to the sink with the aggregate sensory results.

Fig.1 depicts a Secured MA Data Structure, the pair of *Time_Stamp* and *SinkId* is used to identify a MA. We added the sink's public key to the sink Id field and the SrcList will include the public keys of source nodes along with their identities in this manner {(Sa,PUa), (Sb,Pub)} and so on.

NextSrc denotes the next source to be visited. After processing the sensory data on a source node, the MA will delete the corresponding ID from the SrcList. *SrcNum* denotes the number of IDs remaining in the *SrcList*.

Time_Stamp	SinkID+PU Key	Fst_Src	Lst_Src	Next_Src	SrcList+PU Key	Src Num	Processing Code	Data

Figure 1: Secured Mobile Agent Data Structure

Now the sink will encrypt MA with the first source's public key and then dispatch the encrypted mobile agent to the target region. First source on receiving the MA decrypts the it with its private key. *Fst_Src* copies the MA processing code into its memory and the MA starts functioning. MA migrates among target nodes to collect sensory data and also copies its processing code into the memory of each source node.

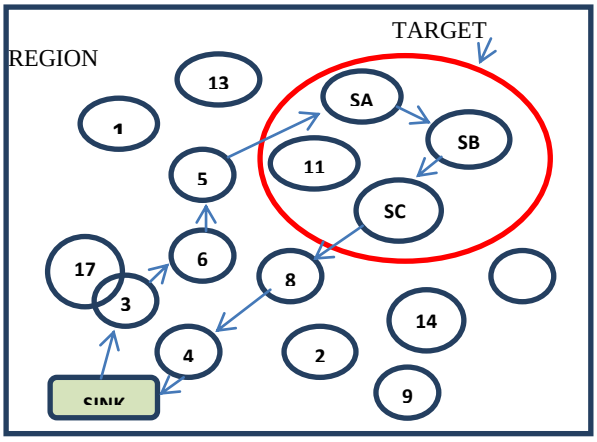

Figure 2: Detailed Mobile Agent action phase

Now, the agent processes the sensed data stored at source node and aggregates it. After processing, source node will encrypt the MA with the next source's public key. Next source on receiving the agent decrypts the MA with its private key and copies the MA processing code into its memory and the MA starts functioning. MA processes the sensed data stored at source node. MA aggregates this processed data with the data stored in agent data field. On the last source node, agent processes the data and aggregates it with the data stored in agent data field. Now last source will encrypt the agent with sink's public key.

After visiting *Lst_Src*, the MA discards the processing code and returns to sink with the collected result. After the MA leaves each source node, all the relevant code stored in each source node will be discarded. When the MA leaves *Lst_Src*, it will return to the sink along the reinforced path (e.g., path SC →8 → 4 → *Sink* in Figure 2).

6. ALGORITHM FOR SDDMA

ALGO_SDDMA (src_lst, fst_src, lst_src, nxt_src)

{
Sink : E(Pu_fst_src(MA))
//After creating an agent, Sink will encrypt the agent with the public key of fst_src
Repeat until (src_node !=lst_src)
{
Src_node : D (Pr_Src_node(MA))
//Src_node , upon receiving the encrypted agent ,decrypt it with its private key
MA : Process(data)
//Agent will process the sensed data, stored at src node
MA : Aggregate(data)
// Agent will aggregate the processed data with its data
Src_node : E(Pu_nxt_src(MA))
// src node will encrypt the agent with nxt_src public key and send the agent to next node
Send(E(MA)) to nxt_src
}
MA : Process(data)
//Agent will process the sensed data, stored at last node
MA : Aggregate(data)
// Agent will aggregate the processed data with its data
Lst_src : E(Pu_sink(MA))
//At lst_src after processing,lst_src will encrypt it with the public key of sink.
Sink : D(Pr_sink(MA))
//On receiving, sink will decrypt agent with its private key and achieved the requested data
}

Figure 3: Algorithm for SDDMA

7. FLOWCHART OF SDDMA

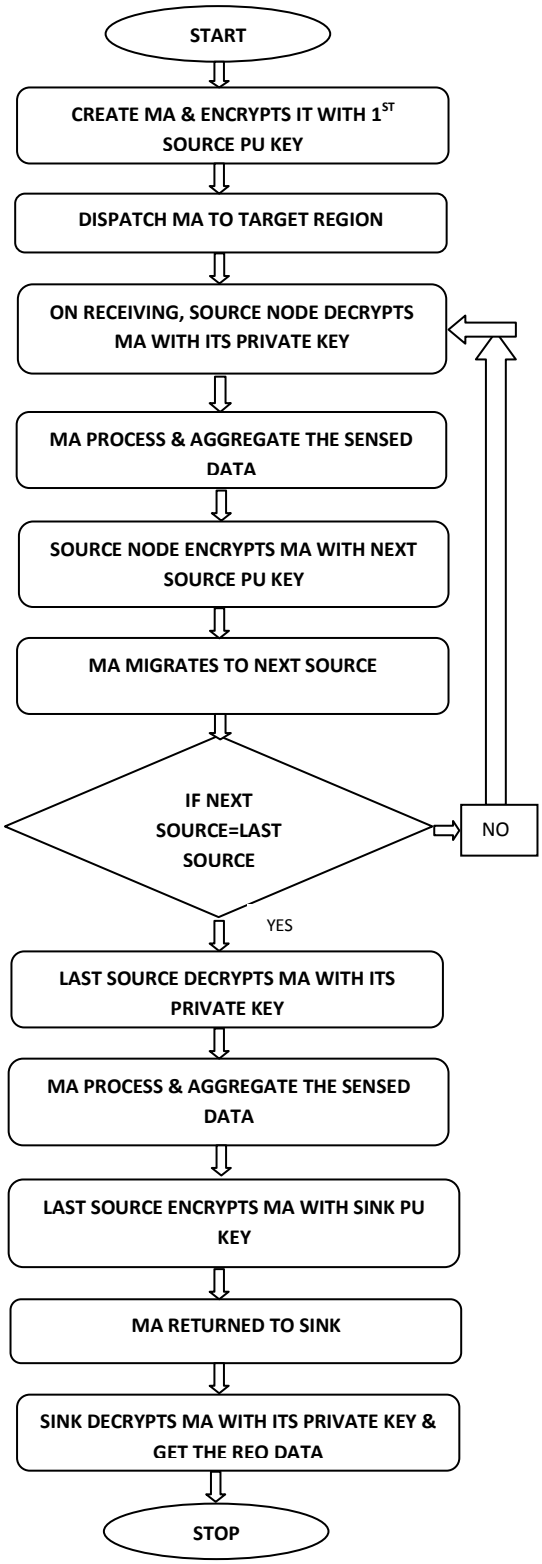

Figure 4: Flowchart of SDDMA

8. CONCLUSION AND FUTURE SCOPE

The purpose for the development of Secured Directed Diffusion using Mobile Agent(SDDMA) is to provide security to the data sent to the sink. It is based on an improved gradient generation algorithm for WSNs called IDDMA. A mechanism is proposed for securely sending the data from source nodes to sink using Mobile Agents. An asymmetric key encryption technique is used for this. For generating the public key and private key pair, RSA algorithm is used.

SDDMA operates in three phases. Using this technique MA is able to process the data, confidentially. Also aggregation takes place at each node while maintaining the confidentiality of the data.

Source node energy is utilized in encrypting and decrypting the agent. All processing and aggregation work is done by the agent which results in saving the energy of the nodes.

In addition, the nodes do not send the sensed data to other nodes, as the agent is taking the data with it. As a result it is also saving much energy of the source nodes.

The recent developments and advancements in wireless sensor networks have opened up the numerous research areas in different fields. Incorporating agent technologies into wireless sensor network shall make them self-organizing, self managing intelligent communities.

Possible future research for SDDMA includes

- The consideration of nodes with heterogeneous capability. Sensor nodes consider so far in SDDMA are homogenous in nature.
- Other open issue for SDDMA is the consideration of mobility of sensor nodes. SDDMA assumes that all the source node in the target region are stationary in nature. For mobile source nodes some extra efforts are needed.

9. REFRENCES

[1] Fei Jiang, Haoshan Shi, Zhiyan Xu, Xiangjun Dong "Improved Directed Diffusion-Based Mobile Agent Mechanism for Wireless Sensor Networks" IEEE, Aug. 2009.

[2] Chalermek Intanagonwiwat, Ramesh Govindan, Deborah Estrin, John Heidemann, and Fabio Silva **"**Directed Diffusion forWireless Sensor Networking" Defense Advanced Research Projects Agency under grant DABT63-99-1-0011.

[3] Kemal Akkaya *, Mohamed Younis "A survey on routing protocols for wireless sensor networks" Elsevier B.V., 2003

[4] Hongjoong Sin, Jangsoo Lee, Sungju Lee, Seunghwan Yoo, Sanghyuck Lee, Jaesik Lee, Yongjun Lee, and Sungchun Kim"Agent-based Framework for Energy Efficiency in Wireless Sensor Networks" World Academy of Science, Engineering and Technology 46, 2008

[5] Nick Jennings,Michael Wooldridge" Software Agents" IEE Review, pp 17-20, January 1996.

[6] Yashpal Singh1 ,Kamal Deep2 and S Niranjan3 "Multiple Criteria Clustering of Mobile Agents in WSN" International Journal of Wireless & Mobile Networks (IJWMN) Vol. 4, No. 3,

[7] Wang Jietai, Xu Jiadong, Yang Shaojun "Research on Mechanism of Mobile Agent for Wireless Sensor Networks" IEEE, 2007.

[8] Suat Ozdemir,, Yang Xiao "Secure data aggregation in wireless sensor networks: A comprehensive overview" Elsevier B.V., 2009.

[9] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong "Security in Wireless Sensor Networks: Issues and Challenges", ICACT, pp. 20-22, Feb. 2006.

[10] Mitsuru Oshima,Guenter Karjoth "Aglets Specification (1.0)" IBM May 20th, 1997

[11] S. John, "Wireless Sensor Networks," Department Of Computer Science, University Of Virginia , June 19, 2006.

[12] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "A survey on sensor networks" IEEE Commun. Mag. Vol. 40 no. 8, pp. 102–114, 2002.

[13] K. Akkaya, M. Demirbas, R.S. Aygun, "The Impact of Data Aggregation on the Performance of Wireless Sensor Networks" Wiley Wireless Commun. Mobile Comput. (WCMC) J. 8, pp. 171–193, 2008.

[14] R. Rajagopalan, P.K. Varshney, "Data aggregation techniques in sensor networks: a survey" IEEE Commun. Surveys Tutorials, vol. 8, no. 4, 2006.

[15] B. Krishnamachari, D. Estrin, S. Wicker, "The impact of data aggregation in wireless sensor networks" Proceedings of the 22nd International Conference on Distributed Computing Systems Workshops, pp. 575–578, 2002.

[16] J. N. Al-Karaki and A. E. Kamal, "Routing techniques in wireless sensor networks: a survey," IEEEWireless Communications, vol. 11, no. 6, pp. 6–28, 2004.

[17] L. Szumel, J. LeBrun, J. D. Owens, "Towards a Mobile Agent Framework for Sensor Networks," Proc. 2nd IEEE Workshop on Embedded Networked Sensors, Sydney, Australia, pp .79–88, 2005.

[18] D. Culler, D. Estrin, M. Srivastava, "Overview of sensor networks," IEEE Computer, vol. 37, no. 8, August 2004.

[19] V. Kunchakarra, "simulation study of routing protocols in wireless sensor networks," Department of Computer Science, Osmania University, Dec. 2005.

[20] S. Misra et al. (eds.) "Guide to Wireless Sensor Networks Computer Communications and Networks" DOI: 10.1007/978-1-84882-218-4 4, Springer-Verlag London Limited, 2009.

[21] Chandrakasan, A., Rabiner Heinzelman, W., Balakrishnan, H.: "Energy efficient communication protocols for wireless microsensor networks".33rd Hawaii Int. Conf. on Systems Sciences, vol. 2, pp. 3005–3014, January 2000.

[22] Boulis, A. et al. "Aggregation in sensor networks: An energy - accuracy tradeoff." IEEE workshop on Sensor Network Protocols and Applications, 2003.

[23] Akyildiz, I. et al. " Wireless sensor networks: a survey". Elsevier Computer Networks, 38, 2002