ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)
On 21st & 22nd March Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

Protecting Privacy Secure Mechanism for Data Reporting In Wireless Sensor Networks

V V.Rithun[#1], C.Senthil Kumar[*2]

[#1]PG student, Department of Information Technology, SNS College of Technology, Coimbatore, Tamil Nadu, India.

[*2]Assistant Professor, Department of Information Technology, SNS College of Technology, Coimbatore, Tamil Nadu, India.

***Abstract*—**Wireless sensor networking is an emerging technology, which potentially supports many emerging applications for both civilian and military purpose. Node compromise is the major and unique security issues in sensor network. These compromised nodes could report false sensed results and degrade the reliability of the whole network. The secure network protocol of motesec aware only provide security against DoS attack with AES and to detect the replay and jamming attacks based on synchronized incremental counter approach. But the false report injection attacks will not be detected in motesec aware. The false report injection is one of the critical threats in wireless sensor network. Sometimes it may destroy the whole network. Filter the false report injection attacks and to prevent dos attacks dynamic en-route filtering scheme is used. The scheme each node has a hash chain of authentication keys used to endorse reports mean while a legitimate report should be authenticated by a certain number of nodes. Finally we prove our scheme efficient than existing work in terms of energy consumption and communication overhead also provide security by early detection of false reports.

***Index Terms*—** Data reporting, Dynamic en-route filtering scheme, wireless sensor networks, security**.**

I. INTRODUCTION

A wireless sensor network is a spatially distributed autonomous sensor to monitor physical or environmental conditions which co-operatively pass their data through the network to a main location. Wireless sensor network contains large number of resource limited sensor nodes each sensor nodes work together and transport useful information to users. One of the main important thing is security and privacy corresponding to data reporting must be concerned that cannot be ignored. Sensor networks may suffer various types of malicious attacks. False report injection attack is one of the attacks that degrade the reliability of whole network.

In the false report injection attack opponent inject false data report into sensor networks. It consists of false data or faked readings from compromised nodes. These types of attacks send unwanted reports to base station and also drain out the limited energy of forwarding nodes. So it is very important to implement a dynamic filtering scheme to filter these types of attacks. Security is one major challenging issue in wireless sensor networks. In the existing work there are many security mechanism is developed. It consists of some the disadvantages. To overcome the disadvantages of existing system we propose a dynamic en-route filtering scheme to filter the data report whether it contains the injected false data reports. By using this filtering scheme we can provide a secure mechanism for data reporting in wireless sensor networks. The paper is organized as follows. We launch the network model in Section II and define the existing work in Section III. In Section IV we present our proposed work. Simulation results are discussed in Section V. Finally we conclude the paper with Section VI.

II. NETWORK MODEL

Sensor nodes are organized into clusters. The deployed sensor nodes form a number of clusters and each cluster consist of cluster head. The sensor nodes sense the data and send the data to corresponding cluster head. Through this way the sensor node can balance energy

consumption. Sensor node detecting the events are called sensing nodes. They create and broadcast the data report to the cluster head.

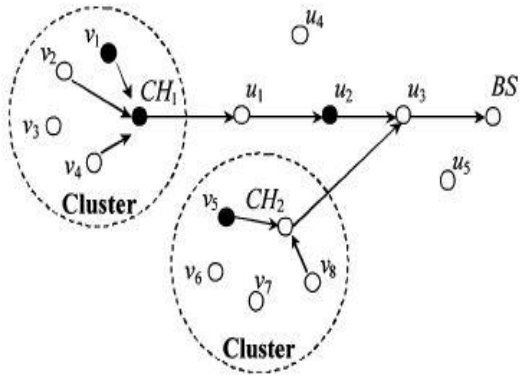

Fig.1 Sensor nodes organized into clusters.

Cluster head collect all the broadcast data report and forwarding these data report to the base station through some forwarding nodes. Fig.1 illustrates the network model of sensing nodes. In the figure big dashed circles outline is the region of clusters. CH and BS denote as Cluster Head and Base Station. Forwarding nodes are denoted as $u_1,u_2\ldots\ldots u_5$ and sensing nodes are $v_1,v_2\ldots\ldots v_8$. The black color dots are representing the compromised nodes and they are located either within the clusters or en-route. When some events occurs the sensor node sense the events and send to the cluster head. Event can detect at least *t* number of nodes. Sensor node creates and broadcast the sensing reports to the cluster head. The cluster head collects all the sensing reports and finalize to the aggregated reports and forwarded to base station through some forwarding nodes.

In this paper we are providing a secure mechanism for data reporting in wireless sensor network through identifying the false data report. Due to the mobility of the nodes the topologies of wireless sensor networks change frequently this cause fail to detect the false data to overcome this a dynamic en-route filtering scheme is applying here.

In this paper we think about the following attacks launched by the opponent from the compromised nodes:

False report injection attacks: In false report injection attacks the compromised nodes can send the false reports containing nonexistent events occurring in their clusters. These false data report drain out the limited energy of forwarding nodes and also cause false alarm at the base station.

III. EXISTING WORK

A. Overview

In the existing work it explains about the security mechanism for wireless sensor network. Motesec-aware is a practical secure mechanism for wireless sensor network [1]. It provides a high security mechanism with low energy consumptions. In this paper it identify the various attacks and it mainly focus on data access control and secure network protocols. A virtual counter manager with a synchronized incremental counter is presented to detect the replay attack. Jamming attack is identified using symmetric key cryptography AES in OCB mode. It also prevents unauthorized accesses by using Key-Lock Matching method. Through identifying the various it can achieve the goals of much less energy consumption. A. Perrig, R. Szewczyk and J.D. Tygar present a security protocol for sensor networks. It mainly provides the data confidentiality, two party data authentication and data freshness. SPINS achieves low energy consumption and also provide security for wireless sensor networks [2]. C. M. Yu, Y.T. Tsou, C. S. Lu and S. Y. Kuo proposed the Constrained Function based message authentication scheme for wireless sensor networks. CFA is the first authentication scheme supporting en-route filtering with only a single packet overhead. In this paper it mainly concentrates on authentication in sensor networks [3]. It does not focus on data reporting in wireless sensor networks. F. Ye, H. Luo, S. Lu, and L. Zhang proposed a statistical en-route filtering scheme to identifying the false data report. It is based on probabilistic key distribution. This filtering scheme is not applicable for dynamical environment [4]. The filtering scheme is only applicable in the statistical environment. Zhu et al. present an interleaved hop by hop authentication scheme for filtering of injected false data in sensor networks. It also provides the security in sensor through identifying the false data [5]. Giruka. V. C and Singhal.M explain about the security issues and possible attacks in wireless sensor networks. It mainly focused on authentication, key management and distribution, secure routing, denial of service, and intrusion detection [6]. Yu.C.M, Lu.C.S, and Kuo S.Y present a DoS Resilent en-route filtering scheme for sensor networks to identify the false data injection attack and also defending against PDoS, FEDoS and FIDoS attacks and also it maximizing the resilience to dynamic topology [7].

S. Kun and M. Douglas proposed a prototype of secure network access control system in wireless sensor networks [8]. The security mechanism for data aggregation in wireless sensor network is also introduced in SIA [9]. It also introduces the secure mechanism for distributed access control in sensor networks [10]. Z. Yu and Y. Guan present a dynamic en-route filtering scheme for identifying the injected false data. It provides a security through identifying the false data that a compromised node can send [11]. TinySec is a secure sensor network link layer protocol. It achieves low energy consumption by reducing the level of security in sensor networks [12]. S. Zhu and S. Setia presented a security mechanism for large-scale distributed sensor networks (LEAP) [13]. A commutative cipher based en-route filtering scheme is used to filter the false reports generated by a malicious node [14]. C. Karlof and D. Wagner proposed a routing security in wireless sensor networks. The authors introduce two novel classes of previously undocumented attacks against sensor networks [15]. It does not provide a security against data reporting in sensor networks. There are many existing work presented about the security toward resilient [16] and

secure multidimensional query (SMQ) schemes for sensor network [17]. These all existing work presented only the security for sensor networks through identifying the various attacks. It does not concentrated on the efficient data reporting in the wireless sensor networks.

B. Problem Identification

In existing work the main drawback is efficiency to filtering the data is very low and false report injection attack could not be filtered and verified. The compromised nodes can send the false reports containing some forged or non existing events occurring in their clusters. These false reports not only cause false alarm at the base station and also exhaust out the limited energy of forwarding nodes. Because of the mobility the false report injection attack is more challenging and hard to resist.

IV. PROPOSED WORK

We propose a dynamic en-route filtering scheme for detecting injected false data report. When the events occur the sensor node collects all the event and send to corresponding cluster head. Cluster head aggregate to aggregate reports forwarded to the base station through forwarding nodes. In our scheme contains three phases Key Pre-Distribution, Key Dissemination, Report Forwarding.

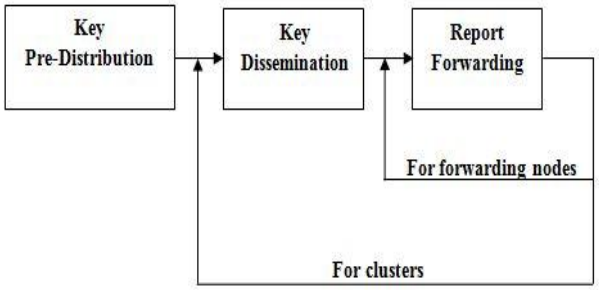

Fig.2 The relationship between three phases.

The fig.2 illustrate the three phases of dynamic en-route filtering scheme. Key pre-distribution is performed only once. The clusters are executed keydissemination periodically. Report forwarding happens at each node in every round. In our scheme each sensor node hold a sequence of authentication keys (auth-keys) that form the hash chain. Cluster head spread the first auth-keys of all sensor nodes to the forwarding nodes before sending the data reports. In wireless sensor network the forwarding nodes are situated on multiple paths between the cluster head and base station. The data reports are organized into rounds that contain a fixed number of reports. Sensing node pick a new auth-key to authenticate its data reports for an each round. To easy verification of the forwarding nodes the sensing node opens up their auth-key at the end of each round. Forwarding node can receive the open up auth-keys only when its upstream node overhears that it has already broadcast the data reports. Each forwarding node verifies the data reports based on the open up key that have received and informs its nearest neighbor node to forward or drop the data reports depending upon the verification result. The processes of verification are repeated on each forwarding node at every hop before the data reports are dropped or delivered to the base station.

We discuss the functions of each phase in detail.

1) Key Pre-distribution Phase: each sensor nodes is preloaded with a different seed key from which it can generate a hash chain of its auth-keys.

2) Key Dissemination Phase: the cluster head distribute each sensor nodes first auth-key to the forwarding nodes. Through this method we can prevent the malicious node attack that inject randomly data reports that contains falsified auth-keys. Based on distributed auth-keys it will be able to filter the false data reports.

3) Report Forwarding Phase: in report forwarding phase the forwarding nodes verifies the data report based on the open up auth-keys and distributed ones. After the verification of the data report if it is valid then the forwarding node sends the data report to its next hope node. The data reports forwarded hop by hop to the base station. At each hop a forwarding node verifies the validity of data reports based on the open up keys and informs the verification result to the its own next hop node. The mechanism is repeated by every forwarding node before the reports are dropped or delivered to the base station.

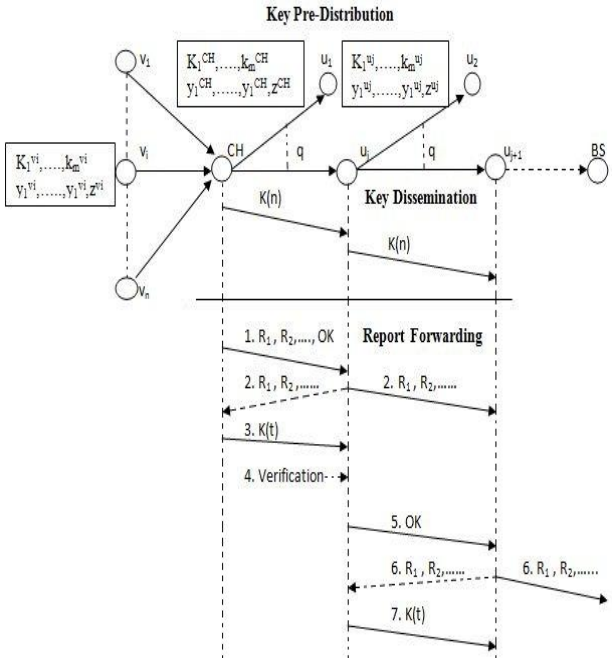

Fig.3 The detailed functions of three phases.

In the fig.3 shows the detailed functions of three phases of dynamic en-route filtering scheme. Sensor node is denoted as $v_1,..,v_i....v_n$ and CH is denoted as cluster head. The forwarding nodes are $u_1,u_2.....u_{j+1}$ and BS denoted as Base station.

Step 1: The cluster head collects the sensing reports from all sensor nodes. Cluster generate set of data reports such as $R_1,R_2,.....$and send to the forwarding node u_j with an OK message. Cluster head distribute a K(n) message that contain auth message of each sensor node to the

forwarding nodes. Each set of data reports contain the t MACs that means the set of data reports containing t number of sensing node reports with different auth-keys (z-keys).

Step2: The forwarding node u_j receives set of data reports and also OK message. Then the u_j forward the set of data reports to the nearest forwarding node u_{j+1}. Cluster head overhears the broadcast of set of data reports from forwarding node u_j.

Step3: When the cluster head overhear the broadcast from u_j it send a K(t) message. K(t) consist of open up auth-keys of each sensor nodes.

Step4: Forwarding node u_j receives the K(t) message. First u_j checks the authenticity of the open up keys using the distributed ones that is decrypted from the K(n) message. By using MACs and open up keys it checks the integrity and validity of the data reports.

The verification processes are:

1) The forwarding node u_j checks the K(t) message whether it contains different z-keys in correct format. If not it drops the message K(t). The verification processes is done for verify the validity of K(t).

2) The forwarding node verify the authenticity of auth-keys in K(t) by using hashing function method.

3) The integrity and validity of the data report is verified by using the open up keys that it decrypted from the message K(t).

Step5: If the data reports are valid then the forwarding node u_j send an OK message to nearest forwarding node u_{j+1} or otherwise the data report is not valid it informs to u_{j+1} to drop the data reports.

Step6: every forwarding nodes repeats the processes until the data report are dropped or delivered to the base station.

These are various procedures for identifying injected false data report.

V. SIMULATION RESULTS

Filtering the injected false data report attack is the main problem in wireless sensor networks. There is many existing mechanism for providing security in wireless sensor networks but it is not efficient for filtering false data report. So a scheme is introduced to filter the injected false data report. These scheme is the dynamic en-route filtering scheme. The dynamic en-route filtering scheme shows the filtering of false data report. Through identifying the injected false data report it provide a high security mechanism for data reporting in wireless sensor networks. Filtering capacity of scheme is defined as the average number of hops that false data report can travel. It is determined by the probability that a false data report can be detected by the forwarding node at every hop. Analyzing the various parameters dynamic en-route filtering scheme is efficient for data reporting in wireless sensor networks.

The comparison graph of various parameters focuses on A. Packet lost ratio, B. Overhead ratio, C. Packet delivery ratio.

A. Packet Lost Ratio

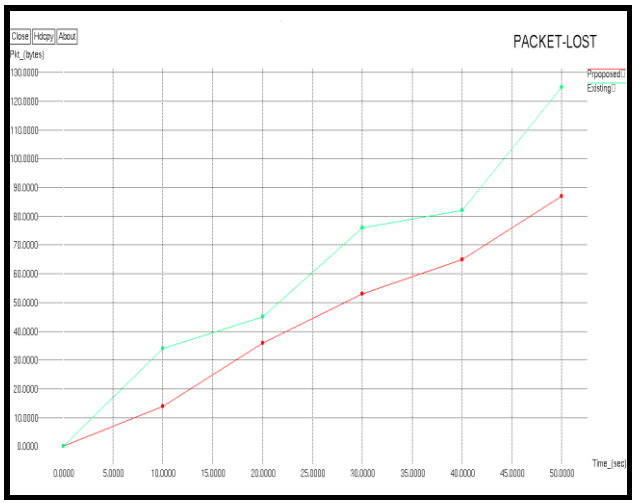

Fig.4 Packet lost ratio

The fig.4 shows the packet lost ratio of proposed scheme and existing scheme. Compare to existing scheme the proposed scheme reduce 40% of the packet lost ratio.

B. Overhead Ratio

The fig.5 shows the overhead ratio of proposed scheme and existing scheme. Compare to existing scheme the proposed scheme has low overhead ratio. It reduces 40% of overhead ratio.

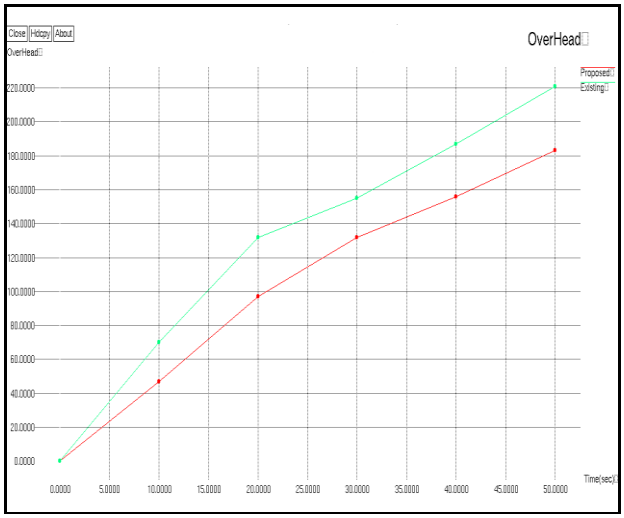

Fig.5 Overhead ratio

C. Packet Delivery Ratio

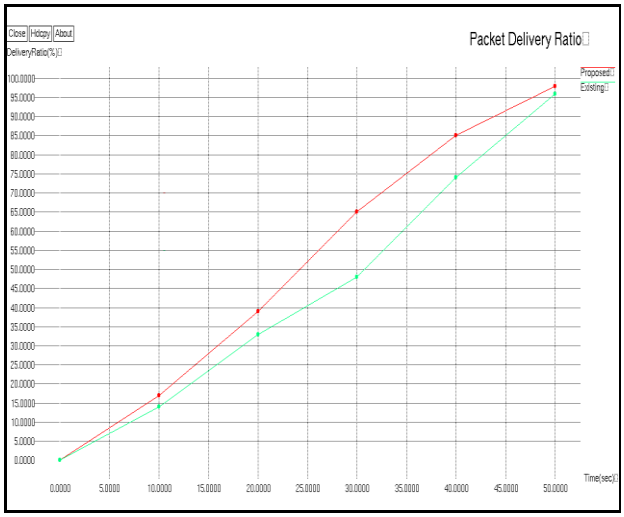

Fig.6 Packet delivery ratio

The fig.6 shows the packet delivery ratio of proposed scheme and existing scheme. Compare to existing scheme the proposed scheme gives 98% of the packet delivery ratio. Comparison results of various parameters shows the dynamic en-route filtering scheme is more efficient than other scheme.

VI. CONCLUSION AND FUTURE WORK

Security is serious for many sensor networks, because of the limited capabilities of sensor nodes. To offer security and privacy to a sensor network is a difficult task. There are many mechanisms which explain about the security for wireless sensor networks. The Motesec aware is one of the secure mechanisms in wireless sensor networks. It provides security in WSN by identifying some of the attacks. One of the drawbacks of Motesec scheme is that it is not efficient for Data Reporting. To improve the efficient data reporting in WSN an efficient dynamic en-route filtering scheme is used here. This filtering scheme is used to filter the information of the compromised node. Through this filtering scheme we can identify the injected false data report attack and provide secure mechanism for data reporting in wireless sensor network. When we identify the false data report it can also reduce the energy consumption and communication overhead. In the future work, the performance of this filtering scheme will be analyzed under different routing protocols.

REFERENCES

[1] Yao-Tung Tsou, Chun-Shien Lu, Sy-Yen Kuo, "Motesec-Aware: a practical secure mechanism for wireless sensor network," IEEE Trans. On Wireless Communications, vol. 12, no.6, pp. 2817-2829, 2013.

[2] C. M. Yu, Y. T. Tsou, C. S. Lu, and S. Y.Kuo, "Constrained function based message authentication for sensor networks," IEEE Trans. Inf. Forensic and Security, vol. 6, no. 2, pp. 407-425, 2011.

[3] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "SPINS: security protocols for sensor networks," in Proc. 2001 International Conference on Mobile Computing and Networking, pp. 189-199.

[4] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route detection and filtering of injected false data in sensor networks," in Proc. IEEE INFOCOM, 2004, vol. 4, pp. 2446-2457.

[5] S. Zhu, S. Setia, and S. Jajodia, and P. Ning, "An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks," in proc. IEEE Symp. Security Privacy, 2004, pp. 259-271.

[6] Giruka. V. C, Singhal.M, Royalty. Y, and Varanasi.S, (2007) "Security in Wireless Sensor Networks," Wireless Comm. and Mobile Computing, vol.8, no. 1, pp. 1-24.

[7] Yu.C.M, Lu.C.S, and Kuo S.Y, (2005) "A Dos-Resilient En-Route Filtering Scheme for Sensor Network," Proc. Tenth ACM Int'l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc'09), pp. 343-344.

[8] S. Kun, L. An, N. Peng, and M. Douglas, "Securing network access in wireless sensor networks," in Proc. 2009 International Conference on Wireless Network Security, pp. 261-268.

[9] B. Przydatek, D. Song, and A. Perrig, "SIA: Secure information aggregation in sensor networks," in Proc. ACM SenSys, 2003, pp. 255-265.

[10] D. He, J. Bu, S. Zhu, S. Chan, and C. Chen, "Distributed access control with privacy support in wireless sensor networks," IEEE Trans. Wireless Commun., vol. 10, no. 10, pp. 3472-3481, Dec. 2011.

[11] Z. Yu and Y. Guan, "A dynamic en-route scheme for filtering false data injection in wireless sensor networks," in Proc. IEEE INFOCOM, 2006, pp. 1-12.

[12] C. Karlof, N. Sastry, and D. Wager, "Tinysec: a link layer security architecture for wireless sensor networks," in Proc.2004 International Conference on Embedded Networked Sensor Systems, pp. 162-175.

[13] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient security mechanisms for large-scale distributed sensor networks," in Proc. ACM CCS, 2003, pp. 62-72.

[14] H. Yang and S. Lu, "Commutative cipher based en-route filtering in wireless sensor networks," in Proc. IEEE VTC, 2004, vol. 2, pp. 1223-1227.

[15] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," in Proc. 1st IEEE Int. Workshop Sensor Netw. Protocols Appl., 2003, pp. 113-127.

[16] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, "Toward resilient security in wireless sensor networks," in Proc. ACM MobiHoc, 2005, pp. 34-45.

[17] C. M. Yu, Y. T. Tsou, C. S. Lu, and S. Y. Kuo, "Practical and secure multidimensional query framework in tiered sensor networks," IEEE Trans. Inf. Forensic and Security, vol. 6, no. 2, pp. 241-255, 2011.

BIOGRAPHY

C. Senthil Kumar is an assistant professor in SNS College of Technology, Coimbatore. He had completed a master degree in Computer Science Engineering from Kumaraguru College of Technology, Coimbatore. His area of interest is Wireless Sensor Networks. He had an industrial experience of 1 year at a reputed software company.