Providing Address Anonymity in Multicast Multi-hop Wireless Sensor Networks

[1]Chitra R, [2]Dr.S.N.Jagadeesha
[1]Assistant Professor, [2]Professor
[1]Department of Information Science Engineering,NIE Institute of Technology, Mysuru, India,
[2] Department of Computer Science Engineering,JNN College of Engineering,Shimoga,India

***Abstract* -Due to the open nature of a Wireless sensor network(WSN),it is relatively easy for an adversary to eavesdrop and trace packet movement in the network, in order to capture the nodes physically. The nodes in WSN can sense, collect and disseminate information for many different types of applications .One of these applications is subject tracking and monitoring, in which monitored objects often need protection, from different adversaries. An adversary might trace the messages in the WSN to find the source node that sent the message. The adversary might try to disrupt the source and the destination node and hence the entire network to fulfill his agenda. Hence the question is :how do we hide the locations of the communicating nodes, from the adversary? This question is relevant in many applications like battlefield surveillance, patient monitoring, etc. In this paper, we discuss the core techniques used to provide location privacy within WSN, in relations to the assumptions about the adversary's capabilities. Further, in this paper we propose a novel anonymity scheme to hide the identities of the nodes that participate in the message transmission.**

***Index Terms* - Address anonymity, Location Privacy, Simple Message Authentication Code(SMAC), Random Routing Scheme(RRS), TinyOS, Cluster Head, Dummy Packet Injection Scheme(DPIS), Anonymous Communication scheme(ACS)**

I. INTRODUCTION

A Wireless Sensor Network (WSN) consists of a large number of autonomous sensor nodes which are spread over a geographical area to monitor environmental and surrounding information. They transmit the sensed data to centralized locations like cluster heads and sink nodes, by wireless communication. From sink nodes, data is transmitted to a base station for further use. Communication also takes place from base station to sink nodes, from sink nodes to cluster heads and then to sensors. Queries and control information are sent to the sensor nodes. WSNs are used in military and civilian applications. Generally sensor nodes, cluster heads and sink nodes are static. A small sized WSN with a point to point multi-hop unicast path from node A to the cluster head is illustrated in Fig.1. TinyOS [1] is a typical operating system for wireless sensor nodes. TinyOS is based on an event-driven programming model

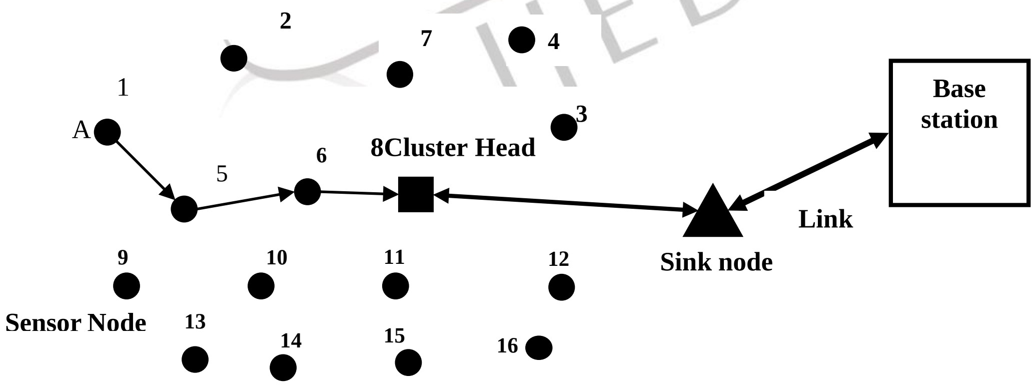

fig.1. a network model

II. ADVERSARY MODEL

An adversary could seize control of several nodes in a network and reprogram them, unknown to the rest of the network. In general, adversaries can be divided into two categories: passive and active. Passive adversaries eavesdrop on communications between sensor nodes in the network. Active adversaries can compromise or physically capture sensor nodes to obtain their data and encryption keys. In our work, we assume that adversaries have both of the above capabilities: an adversary can eavesdrop on all the communications in the network and also capture a limited number of sensor nodes in the network.

A second distinction can be made between outsider attacks and insider attacks. In insider attacks, the adversary is a participant in the sensor network while in outsider attacks, the adversary is not a part of the network.Further discussion can be found in [15]. We provide address privacy and data security against all these attacks.

III. PRIVACY OF SOURCE AND DESTINATION ADDRESSES

When WSNs are deployed in military applications in hostile environments, they are prone to adversarial attacks. The adversaries either steal the data or disrupt the working of the WSNs. The adversaries would like to capture the nodes and through them to control the whole WSN to achieve their agenda. Cluster heads and sink nodes are more vulnerable because they are the critical links in a given WSN. They also carry more information than other nodes and the adversary gains more by capturing the Cluster Heads and sink nodes. A malicious eavesdropper may capture the transmitted data packets, get hold of cryptographic keys and get access to the payload data, source address and destination addresses. Once the true addresses are known their geographical location also can be determined.

IV. PROPOSED METHODOLOGY

We propose three schemes to defend against the traffic analysis attack.

A. Random Routing Scheme(RRS)

Traditional routing cannot protect the location privacy because all packets from the source node are routed along a fixed (shortest) path towards the destination. An adversary is able to move one hop closer to the receiver for each packet overheard. So we propose a routing protocol, which randomizes the routing paths, so that the forwarding directions of packets is not always towards the receiver. So the adversary is frequently deviated towards wrong directions due to randomized routing.

B. Dummy Packet Injection Scheme(DPIS)

The basic idea of dummy packet injection is that whenever a sensor node forwards a packet, in addition to normally forwarding the packet to the next hop, it also transmits a dummy packet to a neighbor that is randomly chosen .Attracted by this dummy packet, the adversary may trace to a wrong direction instead of the real next hop. Each dummy packet has a TTL parameter specifying the maximum number of hops it will be forwarded away from the receiver .When a node receives a dummy packet ,it decrements the TTL field of the packet by one. If the TTL field is positive, the node randomly chooses a neighbor and forwards the dummy packet to that neighbor.

C. Anonymous Communication scheme(ACS)

A privacy problem in WSN is the naming of nodes and base stations. Using the node real ID may be considered as vulnerable, because an adversary is able to identify individual nodes .So the solution is to use some kind of pseudonyms. In this scheme, we propose a technique that prevents exposure of sensor IDs, by using Phantom ID (PID) instead of real Source ID (SID), that makes it difficult for attacker to obtain sensor node data simply by analyzing the traffic. Using this technique only the destination can identify the sensor IDs.

After the initial distribution of sensors ,each sensor creates PID as shown in the expression1.In the neighbor discovery process ,PIDs are exchanged among neighboring sensors.

$$PID=q^{SID} \bmod p \qquad \ldots\ldots\ldots\ldots\ldots\ldots(1)$$

PID is created based on source ID. Going the opposite way or trying to get SID based on PID is made difficult by prime factorization.In addition CRC is replaced with SMAC(Simple Message Authentication Code).The existing MAC technique was modified to be suitable for the sensor network so that only destination sensors are able to identify transmitter sensors accurately and quickly.

SID	Destination ID	Payload	CRC

fig.2.original data frame

PID	Destination ID	Payload	SMAC

fig.3.proposed data frame

V. RELATED WORK

1. Use of pseudonyms and phantom names

One simple way of hiding the identity of a node is to use false names which are also called pseudonyms and phantom names. A false name or id is a name which is markedly different from the true id or name. A pseudonym corresponding to a real name is obtained using a look table or using a complex encryption using appropriate keys.

Misra and Xue [2] have used pseudonyms instead of actual addresses as identities so that the third party cannot make out the real identities. They have proposed two schemes. The first scheme is Simple Anonymity Scheme (SAS) which uses multiple pseudonyms for a node to hide its identity. The communicating nodes in the network share their individual pseudonyms and use them to conceal the true identities of the nodes. Thus the communication is anonymous, and a node’s true ID is kept private. The second scheme is Cryptographic Anonymity Scheme (CAS) which uses cryptographic one way hash functions to conceal the real identities of nodes.

In CAS, a Keyed Hash Function (KHF) is used to generate the pseudonyms. Hence, the pseudonyms cannot be identified nor generated by an outside adversary even if it captures previous messages sent by the sensor node.

Park j et al [3] have proposed a new technique for providing anonymity using Phantom ID and SMAC (Sensor Medium Access Control) which is basically an energy efficient MAC, especially suitable for WSNs. This method assumes that the type of attack against a sensor network is mainly eavesdropping. Dynamically changing pseudonyms are used instead of fixed ones. In this method, the usage of Hidden Vector in the address field provides a more secured address anonymity compared to [2]. The Phantom ID denoted by PID is generated as, PID = q^{SID} mod p, where q and p are large prime numbers and SID is the true ID of the sensor. By knowing PID, the value of SID cannot be determined. This is called the discrete Logarithm problem. Our work is inspired by this paper.

2. Efficient Key Distribution

Efficient Key Management is an essential requirement for any security system. Several techniques have been described by various authors for this.

Perrig A, et al [4] have proposed Security Protocols for Sensor Networks (SPINS), an efficient but low overhead key distribution protocol. SPINS has two components: SNEP (Secure Network Encryption Protocol) and µTESLA (micro Timed, Efficient, Streaming, and Loss-tolerant Authentication Protocol). SNEP provides data confidentiality, two-party data authentication, and evidence of data freshness. µTESLA provides authenticated broadcast for severely resource-constrained environments. SPINS uses a shared master key. All subsequent non repeating keys are generated from this master key. Generally asymmetric key authentication is used in wired communication. But this method is not suitable for sensor networks because of large key size, large memory requirement and complex computational requirements which make up a high overhead. Therefore, symmetric key cryptography is adopted in this work. Here, the sender and receiver share a common counter for easy synchronization and it is automatically incremented after the transmission of the packet at the sender and after receiving the packet at the receiver. This saves the overhead of transmitting the counter value. In this work, Message Authentication Code (MAC) is used for authentication.

3. Address anonymity and prevention of Denial of Service (DOS) attack

Wadaa et al [5] use a dynamic virtual infrastructure constructed on top of the physical sensor nodes to provide anonymity. Polar coordinates are used for the location of sensors. In this method, a training phase and a harvesting phase are set up to provide anonymity for the entire WSN structure. The virtual infrastructure is kept confidential and the adversary cannot inflict Denial of Service (DOS) Attack.

4. Secured Group Communication in WSNs

Pitipatana Sakarindr and Nirwan Ansari [6] discuss the security of WSNs with reference to group communication. In this paper different types of attacks in a WSN are explained in detail. Identity related attacks like impersonation, Sybil attack and traffic analysis related attacks are fully described. This technique provide Secured Group Communication (SGC) security. Group Key Management (GKM) protocol has been proposed by the authors. GKM is categorized into three types as, centralized, distributed, and contributory. All the three types are realized in this work.

5. LPR with fake packet injection

Ying Jian, Shigang Chen, Zhan Zhang and Liang Zhang [7] have proposed a new receiver location-privacy routing protocol, called LPR, to provide path diversity. This routing protocol is combined with fake packet injection to minimize the information that an adversary can deduce from the overheard packets about the direction towards the receiver. This will confuse the adversary. Sensors near the receiver forward a greater volume of packets than sensors further away from the receiver. LPR mitigates the traffic analysis attack. In this type of attack an adversary is able to compute the traffic densities at these locations, based on which it deduces the location of or the direction to the receiver by eavesdropping the packets transmitted at various locations in a sensor network,

6. Random key pre-distribution Scheme

H. Chan, A. Perrig and D. Song [8] have proposed Random key pre-distribution schemes for sensor networks. They have presented 3 mechanisms for initial pre-distribution of keys. These are q-composite random key pre-distribution scheme, multi-path key reinforcement scheme and

Random pair wise keys scheme. The last method provides security to the rest of the network when any node is captured. In this work, an efficient bootstrapping (starting) scheme for efficient key distribution mechanism is provided. This scheme achieves its goal in three phases as initialization phase, key setup phase and key distribution phase and further, provides multi-path key security and it is easily scalable for new additional sensor nodes.

Du W et al [13] describe another key distribution scheme to provide encryption/decryption. The proposed scheme exhibits a nice threshold property; when the number of compromised nodes is less than the threshold, the probability that communications between any additional nodes are compromised is close to zero. This desirable property lowers the initial payoff of smaller-scale network breaches to an adversary and makes it necessary for the adversary to attack a large fraction of the network before it can achieve any significant gain.

7. Localized Encryption and Authentication Protocol (LEAP)

S. Zhu, S. Setia, and S. Jajodia [9] have described LEAP (Localized Encryption and Authentication Protocol), a key management protocol for sensor networks that is designed to support in-network processing. Here the security impact of a compromised node is restricted to its immediate network neighborhood. LEAP supports the establishment of four types of keys for

every sensor node – an individual key shared with the base station, a pairwise key shared with another sensor node, a cluster key shared with multiple neighboring nodes and group key that is shared by all the nodes in the network. The LEAP protocol is designed based on two observations. Firstly, different packet types exchanged among sensor nodes require different security services and second, a single key management scheme may not be suitable for various security requirements. In LEAP, one-way key chains can mitigate the impersonation attack, and a timestamp is used to make keys expired to prevent node capture and Sybil attacks. LEAP has low communication overheads and the scheme is energy efficient.

8.Using Location-based Keys

Y. Zhang, W. Liu, W. Lou, and Y. Fang [10] have proposed location-based keys for designing compromise-tolerant security mechanisms for sensor networks. The geographic locations of the nodes are used to determine keys of the corresponding nodes. Thus the geographic locations are cryptographically embedded in the keys. Based on these keys, they have developed a node-to-node authentication scheme which is not only able to localize the impact of compromised nodes within their vicinity, but also to facilitate the establishment of pairwise keys between neighboring nodes. This scheme has perfect resilience against node compromise, low storage overhead and good network scalability. In this scheme, the techniques of bilinear pairings are used. This scheme provides protection against Sybil, node impersonation and sink hole attacks.

9. Source-Location Privacy using Phantom Routing

C. Ozturk, Y. Zhang, and W Trappe [11] have focused on protecting the source's location by introducing suitable modifications to sensor routing protocols to make it difficult for an adversary to backtrack the origin of the sensor communication. A set of flooding protocols are discussed in the paper. Proper consideration is given for minimum energy consumption. One of the protocols proposed is phantom routing, which protects the source's location. Phantom routing is a two-stage routing scheme that first goes for a directed walk along a random direction to the phantom destination and then takes a route from the phantom source to the sink. Fake messages and fake sources are created to misguide the adversary who wants to track the true source. Phantom routing is achieved using probabilistic flooding.

P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk [12] discuss enhanced phantom routing and also describe the effect of source mobility on source privacy. Under such condition the authors claim that their method is superior to other existing methods. They use sector based directed random walks and hop based directed random walks to create phantom routings. Phantom techniques introduce additional latency because every message is directed to a random location first. However, the tradeoff is reduced security.

L. Lightfoot, Y. Li, and J. Ren [14], proposed a special routing technique to provide adequate source-location privacy with low energy consumption and introduced this technique as the Sink Toroidal Region (STaR) routing. In this technique, the source node randomly selects an intermediate node within a designed STaR area located around the SINK node. The STaR area is large enough to make it unpractical for an adversary to monitor the entire region. Furthermore, this routing protocol ensures that the intermediate node is neither too close, nor too far from the SINK node in relations to the entire network. While ensuring source location privacy, the proposed scheme is very efficient and can be used for practical applications.

C. Karlof and D. Wagner [15] discuss secure routing against various attacks in a sensor network. They have provided five main contributions and proposed threat models and security goals for secure routing in wireless sensor networks, two novel classes of previously undocumented attacks against sensor networks, sinkhole attacks and HELLO floods, attacks against ad-hoc wireless networks and peer-to-peer networks. Detailed security analysis of all the major routing protocols and energy conserving topology maintenance algorithms for sensor networks is discussed. Further, practical attacks against all of them that would defeat any reasonable security goals and discuss countermeasures and design considerations for secure routing protocols in sensor networks is presented.

10.Using Matrix Keys

Yun Zhou A. [16], in his PhD thesis, describes the use of matrix keys for large sensor networks. The author has devoted an entire chapter on key agreement and key distribution in large WSNs and presented the advantages of using matrices in finite field as keys. The technique uses multivariate symmetric polynomials for generating the elements of the matrices.

R. Blom [17] describes the use of matrices in Galois Field (GF) for cryptography. He has presented the Symmetric Key Generation System (SKGS). Here, the individual large sized keys are generated from the short length basic keys obtained from SKGS.

VI. CONCLUSION

Maintaining anonymity of the communicating nodes is vital to the successful deployment of wireless sensor network. In this paper, we study different techniques used to provide location privacy, anonymity and data security. Further ,we proposed a novel approach to provide address anonymity and data security. First, a random routing scheme(RRS) is proposed to provide path diversity. Second, we combine RRS with a dummy packet injection scheme(DPIS) to confuse the adversary by tracing back the forwarded packet to reach the communicating nodes. Finally, an Anonymous Communication scheme (ACS) is proposed to hide the identities of all the nodes that participate in packet transmission. Through security analysis and simulation ,we can see that our proposed scheme can efficiently defend against traffic analysis attacks ,take less delivery time and achieve uniform energy consumption.

REFERENCES

[1] PhilipLevis,TinyOS Programming, Cambridge University Press, 2009

[2] S. Misra and G. Xue, "Efficient anonymity schemes for clustered wireless sensor networks," International Journal of Sensor Networks, vol. 1, no. 1/2, pp. 50–63, 2006.

[3] Park J. H, Jung Y.H, Hoon Ko, Kim J and Jun M. S, ”A Privacy Technique for Providing Anonymity to Sensor nodes in a sensor network,” T.-h. Kim et al. (Eds.): UCMA 2011, Part I, CCIS 150, pp. 327–335, 2011.Springer-Verlag Berlin Heidelberg 2011.

[4] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, “Spins: security protocols for sensor networks,” Wirel. Netw., vol. 8, no. 5, pp. 521–534, 2002.

[5] A. Wadaa, S. Olariu, L. Wilson, M. Eltoweissy, and K. Jones, “On providing anonymity in wireless sensor networks.” in 10th International Conference on Parallel and Distributed Systems (ICPADS 2004), 7-9 July 2004, Newport Beach, CA, USA, 2004, pp. 411–418.

[6] Pitipatana Sakarindr, Nirwan Ansari, “Security Services IN Group Communications OVER Wireless Infrastructure, Mobile Ad Hoc, and Wireless Sensor Networks,” Volume:14 , Issue: 5.
October 2007. pp. 8-20.

[7] Ying Jian, Shigang Chen, Zhan Zhang and Liang Zhang, “Protecting Receiver-Location Privacy in WirelessSensor Networks,” IEEE Communications Society, IEEE INFOCOM 2007 proceedings. pp 1955-1963.

[8] H. Chan, A. Perrig and D. Song, “Random key pre-distribution schemes for sensor networks,” in IEEE Symposium on Security and Privacy, May 2003, pp. 197–213.

[9] S. Zhu, S. Setia, and S. Jajodia, “LEAP: efficient security mechanisms for large-scale distributed sensor networks,” in CCS ’03: Proceedings of the 10th ACM conference on Computer and communications security. New York, NY, USA: ACM Press, 2003, pp. 62–72.

[10] Y. Zhang, W. Liu, W. Lou, and Y. Fang, “Securing sensor networks with location-based keys,” in Wireless Communications and Networking Conference, vol. 4, 2005, pp. 1909– 1914.

[11] C. Ozturk, Y. Zhang, and W. Trappe, “Source-location privacy in energy constrained sensor network routing,” in SASN ’04: Proceedings of the2nd ACM workshop on Security of ad hoc and sensor networks. NewYork, NY, USA: ACM Press, 2004, pp. 88–93.

[12] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, “Enhancing source location privacy in sensor network routing,” in ICDCS ’05: Proceedings of the 25th IEEE International Conference on Distributed Computing Systems (ICDCS’05). Washington, DC, USA: IEEE Computer Society, 2005, pp. 599–608.

[13] Du,W., Deng, J., Han,Y.S., Varshney, P.K., Katz, J. and Khalili, A. ‘A pairwise key pre distribution scheme for wireless sensor networks’, ACM Transactions on Information Systems
Security, (2005) ,Vol. 8, No. 2, pp.228–258.

[14] L. Lightfoot, Y. Li, and J. Ren, “Preserving source-location privacy in wireless sensor network using star routing,” in 2010 IEEE Global Telecommunications Conference, ser. GLOBECOM 2010, IEEE. Piscataway, USA: IEEE communications society, 12 2010, pp. 1–5.

[15] C. Karlof and D. Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures,” Proc. 1st IEEE Int’l. Wksp. Sensor Network Protocols and Applications (SNPA’03),May 2003.

[16] Yun Zhou A, “security in wireless sensor networks,” A Dissertation presented to the graduate school Of the university of Florida in partial fulfillment Of the requirements for the degree of Doctor of philosophy University of Florida 2007.

[17] R. Blom, “An optimal class of symmetric key generation systems," Proceedings of Advances in Cryptology: EUROCRYPT'84, Paris,France,Apr.1984, pp.335-338.