© 2018 IJSRST | Volume 4 | Issue 7 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Wireless Sensor Networks with Secure Contact Method to Maintain Ambiguity

R. Hamsa Veni[1], P. Prathap[2], P. Balachandra[3]

[1]Assistant Professor, Department of MCA, Sri Venkateswara College of Engineering and Technology, Chittoor, Andhra Pradesh., India

[2-3]PG Scholar, Department of MCA, Sri Venkateswara College of Engineering and Technology, Chittoor, Andhra Pradesh., India

ABSTRACT

In wireless sensor networks it's becoming a lot of and a lot of necessary for sensor nodes to maintain namelessness whereas act data as a result of security reasons. Anonymous communication among sensor nodes is very important, as a result of sensor nodes wish to conceal their identities either being a base station or being a supply node. Anonymous communication in wireless sensor networks includes various necessary aspects, as an example base station namelessness, communication association namelessness, and supply node anonymity. From the literature, we will observe that existing namelessness schemes for wireless sensor networks either cannot notice the complete anonymities, or they're full of various overheads like huge memory usage, complex computation, and long communications. This paper is presenting AN economical secure anonymity communication protocol (SACP) for wireless sensor networks that may notice complete anonymities providing minimal overheads with relevance storage, computation and communication prices. The given secure namelessness communication protocol is compared with varied existing namelessness protocols, and the performance analysis shows that our protocol accomplishes all 3 anonymities: sender node anonymity, base station anonymity, and communication association anonymity while using very little memory, low communication price, and small computation costs.

Keywords : Anonymity, Wireless, Security, Identity, Sensor Nodes

I. INTRODUCTION

Anonymity in sensor networks means preventing a third party other than the message sender and the base station knowing the identity of the two primary parties in a communication. It includes sender anonymity, receiver anonymity, and unlinkability between the sender and receiver. Thus, an adversary cannot determine the sender and receiver's identities through reading a message intercepted from the network or through reading messages forwarded by a sensor node it has compromised, and the adversary also cannot determine whether two communication segments (i.e., message transmissions between two neighboring nodes) belong to the same communication between a sensor and the base station. Anonym zing sensor nodes can confuse adversaries about which sensor is the real sender of a message. To protect the real ID of each sensor, pseudonyms can be used for sensor nodes instead of real IDs; however, using fixed pseudonyms cannot prevent leaking identity information of sensor nodes because a long term passive eavesdropper can deduce the topology of the network through traffic analysis. Misra et al. proposed two anonymous schemes for clustered wireless sensor networks. They proposed to use a pool of pseudonyms for a sensor node to select randomly from them when it is sending messages, and also proposed a Cryptographic Anonymity Scheme (CAS)

in which the pseudonym of a sensor node is generated from keyed hash functions. The two schemes can both provide anonymity under the assumption. That the secret keys shared by sensor nodes and the base station cannot be compromised. However, since many sensor networks are deployed in malicious environments, we need to consider the consequences of key compromise and how to protect the anonymity of sensor nodes even when their secret keys are compromised. In this paper, we propose two methods based on one-way keyed hash chains: Hashing based ID Randomization (HIR) and Reverse Hashing ID Randomization (RHIR). They can provide more anonymity to a sensor node even when its shared secret keys are compromised

Proposed system:-

NETWORK ARCHITECTURE AND FUNCTIONING

In the given sensor network there are hundreds of low end wireless sensor nodes those are uniformly and randomly distributed over a given area of interest. There is one base station and it gathers sensed data from the sensor nodes. The invader nodes have higher competencies than sensor nodes in the given network. The invader nodes have global overhearing capabilities and they can also compromise some sensor nodes of the given network and can initiate active attacks. Explicitly, the invader nodes have ample energy supply, higher computation ability, and more memory. Having such capabilities, the invader nodes could compute arrival angle and could measure the signal strength of the data packets to find the location of source sensor node.

Notation	Explanation
X	Total numbers of node in the network
$Hop_{i,BS}$	Shortest path route (hop counts) from node i to the base station
$D_{i \mapsto j}$	Data communication from node i to neighbor node j
$Key_{i,BS}$	A pair-wise shared key between node i and the base station
$Key_{i,N}$	A pair-wise shared key between node i and neighbor node N
$UA_{ID,i}$	Universal anonymous ID for node i
$BA_{ID,i}$	Broadcast anonymous ID for node i
$HIA_{ID,i \leftrightarrow j}$	One hop anonymous identity shared between node i and node j
E_{Kevi}	Encryption function used by node i
H_1, H_2	Hash functions used
$data$	Data that is sent from source node i
$Key_{i \mapsto j}$	A pair-wise shared key between node i and neighbor node j to decrypt the data
$Key_{i,B}$	key shared by node i while broadcasting

Table I: Notations in Use

The invader nodes when work together in the given network, they could launch passive attack over the network by collectively invading upon the data communication among authentic sensor nodes. The invader could also launch an active attack by physically capturing the authentic senor nodes and write or modify their code to execute Denial of Service (DoS) or replay and forging attacks. The compromised nodes could be anywhere in the given network. Although, there cannot be too many compromised nodes, since there are various schemes to detect such attacks and the given network can take defensive measures to resolve such situation. Table I represent some of the notations used for secure anonymity communication protocol.

The invader nodes when work together in the given network, they could launch passive attack over the network by collectively invading upon the data communication among authentic sensor nodes. The invader could also launch an active attack by physically capturing the authentic senor nodes and write or modify their code to execute Denial of Service (DoS) or replay and forging attacks. The compromised nodes could be anywhere in the given network. Although, there cannot be too many

compromised nodes, since there are various schemes to detect such attacks and the given network can take defensive measures to resolve such situation. Table I represent some of the notations used for secure anonymity communication protocol.the route to the base station. The sensor nodes now compute two anonymous IDs, one universal anonymous ID, *UAID,i* and another broadcast anonymous ID, *BAID,i*. The universal anonymous ID and broadcast anonymous ID are computed as given in (1) and (2) respectively using XOR operation.

$$UA_{ID,i} = H_1 (Key_{i,N} \oplus ID_i) \quad (1)$$

$$BA_{ID,i} = H_1 (Key_{i,B} \oplus ID_i) \quad (2)$$

Now node *i* shares data with its one hop neighbors *j* those are on the route to base station *<FFFF, hop=1, IDi, Keyi,BS, Keyi,N, Hopi,BS>*, where FFFF signifies broadcast message, hop=1 means message is for one hop neighbors, *Hopi,BS* is for the minimum number of hops between sensor node *I* and the base station. Node *j* replies back to node *i*, node *i* then calculates pair-wise key *Keyi↔ j* from node *i* to node *j* as given in (3).

$$Key_{i \leftrightarrow j} = H_2 (Key_{i,j} \oplus Key_{j,i}) \quad (3)$$

Now node *i* create another anonymous ID, *H1AID,i↔ j*, one hop anonymous identity shared between node *i* and node *j*. It is computed as follows:

$$H1A_{ID,i \leftrightarrow j} = H_1 (Key_{i,N} \oplus Key_{N,j}) \quad (4)$$

ANONYMOUS COMMUNICATIONS:-

The following procedure is followed to maintain complete anonymity during data communication:

Once the network is initialized and a sensor node have some data to be communicated to the base station, that is multi-hops away, the source node uses its universal anonymity ID, *UAID,i*, for communicating this data and modifies its universal anonymity ID after each data forwarding. Therefore, the source node, *i*, has to choose the next hop neighbor, *j*, to forward the data, *data*, to the base station in the following format:

$$D_{i \rightarrow j} = H1A_{ID,i \leftrightarrow j} \| E_{Keyi \leftrightarrow j} (UA_{ID,i} \| E_{Keyi} (data) \| H_1 (UA_{ID,i} \| E_{Keyi} (data))) \quad (5)$$

Now the node *i* updates $UA_{ID,i}$ and $H1A_{ID,i \leftrightarrow j}$ as given in (6) and (7).

$$UA_{ID,i} = H_1 (Key_{i,N} \oplus UA_{ID,i}) \quad (6)$$

$$H1A_{ID,i \leftrightarrow j} = H_1 (Key_{i \leftrightarrow j} \oplus H1A_{ID,i \leftrightarrow j}) \quad (7)$$

If some global invader, who is in the neighborhood of node *i* and *j*, observers this data transmission as given in (5), then this invader cannot find who the sender node is or who the receiver node is! Since data communication *Di→j* in (5) is not carrying any information about the node identity and if *j* happens to be the base station, then base station decrypts the *Di→j* with *Keyi→j* to find the *UAID,i*. If the receiver node is a node other than base station.

then periodic random delay for each forwarded message is added so that eavesdropper cannot calculate the timing to find the source node and the destination node. So now base station is the only node that knows the source node with anonymity ID, *UAID,i*. The base station even knows the key to extract the data, *data*. The base station also updates node *i*'s universal anonymity ID, *UAID,i* to its new ID in its neighbor tables for future communications from node *i*.

Conclusion

This paper presents a secure obscurity communication protocol (SACP) for wireless detector networks that may notice complete anonymities. Anonymous communication among detector nodes is important, as a result of detector nodes wish to hide their identities either being a base station or being a source node. Anonymous communication in wireless detector networks includes various vital aspects. Various existing obscurity protocols don't show complete anonymities and a few protocols suffer from overheads like huge storage, complex computation, and long communications. The given, SACP obscurity

protocol is compared with numerous existing obscurity protocols, and also the performance analysis shows that it achieves all 3 anonymities: sender node obscurity, base station obscurity, and communication association obscurity. It is also showing nominal overheads on memory utilization, computation value and communication prices.

II. REFERENCES

1. J Shi, R. Zhang, Y. Liu and Y. Zhang, "Prisense: privacy-preserving data aggregation in people-centric urban sensing systems," in Proc. of the IEEE INFOCOM 2010, San Diego, CA, March 2010.
2. X Chen, K. Makki, K. Yen and N. Pissinou, "Sensor network security: a survey, " IEEE Communications Surveys and Tutorials, vol. 11, no. 2, pp. 52-73, 2009.
3. IF. Akyildiz and E.P. Stuntebeck , “Wireless Underground Sensor Networks,” IEEE Journal on Selected Areas in Communications, vol. 4, no. 6, pp. 669-686, 2008.
4. J Chen, B. X. Fang, L. H. Yin and S. SU, "A Source-Location Privacy Preservation Protocol in Wireless Sensor Networks Using Source-Based Restricted Flooding," Chinese Journal of Computers, vol.33, no. 9, pp. 1736-1747, 2010.
5. J P. Sheu, J. R. Jiang and C. Tu, "Anonymous Path Routing in Wireless Sensor Networks," in Proc. of IEEE International Conference on Communications (ICC’08), 2008.
6. N. Patwari, J.N. Ash, S. Kyperountas, A.O. Hero, R.L. Moses and N.S. Correal, "Locating the nodes: cooperative localization in wireless sensor networks," IEEE Signal Processing Magazine, vol. 22, no. 4, pp. 54-69, 2005.
7. L. Kang, "Protecting location privacy in large-scale wireless sensor networks," in Proc. of IEEE International Conference on Communications (ICC'09), 2009.
8. Y. Yang, M. Shao, S. Zhu, B. Urgaonkar and G. Cao, "Towards event source unobservability with minimum network traffic in sensor networks," in Proc. of the first ACM Conference on Wireless Network Security, 2008.
9. T Chen and S. Zhong, "INPAC: An enforceable incentive scheme for wireless networks using network coding," in Proc. of the 29th conference on Information communications (INFOCOM'10), 2010.
10. A.M. Kermarrec and G. Tan, "Greedy geographic routing in large-scale sensor networks: a minimum network decomposition approach," in Proc. of the eleventh ACM international symposium on Mobile ad hoc networking and computing, 2010.
11. A. A. Nezhad, A. Miri and D. Makrakis, "Location privacy and anonymity preserving routing for wireless sensor networks," Journal of Computer Networks, vol.52, no.18, pp.3433-3452, 2008.
12. M. Shao, Y. Yang, S. Zhu, and G. Cao, "Towards Statistically Strong Source Anonymity for Sensor Networks," in Proc. of IEEE INFOCOM 2008, pp. 51-55, 2008.
13. J. C. Kao and R. Marculescu, "Real-time anonymous routing for mobile ad hoc networks," in Proc. of IEEE Wireless Communications and Networking Conference (WCNC’07), 2007.
14. Y. Zhang, W. Liu and W. Lou, "Anonymous communications in mobile ad hoc networks," in Proc. of the 24th conference on Information communications (INFOCOM'05), 2005.
15. Y. W. Law, J. Doumen and P. Hartel, "Survey and benchmark of block ciphers for wireless sensor networks," ACM Transactions on Sensor Networks (TOSN), vol. 2, no. 1, pp. 65-93, 2006.
16. S. Misra and G. Xue, "Efficient anonymity schemes for clustered wireless sensor networks," International Journal of Sensor Networks, vol.1, no. 1, pp.50-63, 2006.

17. T. Li, M. Song and M. Alam, "Compromised sensor nodes detection: A quantitative approach," in Proc. of the 28th International Conference on Distributed Computing Systems Workshops, 2008.
18. H. Song, L. Xie, S. Zhu and G. Cao, "Sensor node compromise detection: the location perspective," in Proc. of the 2007 international conference on Wireless communications and mobile computing, 2007. [19] R. Lu, X. Lin, C. Zhang, H. Zhu, P.H. Ho and X. Shen, "AICN: an efficient algorithm to identify compromised nodes in wireless sensor network," in Proc. of the IEEE International Conference on Communications(ICC'08), 2008.
19. Y. Zhang, W. Liu, W. Lou and Y. Fang, "Location-based compromise-tolerant security mechanisms for wireless sensor networks," IEEE Journal on Selected Areas in Communications, vol.24, no.2, pp.247-260, 2006

Author's Profile:

R. Hamsaveni working as an Assistant Professor in Sri Venkateswara College of engineering and technology, Chittoor, A.P.

P.Prathap received the P.G degree from Sri Venkateswara College of engineering and technology, Chittoor, A.P in 2018.

P.Balachandra received the P.G degree from Sri Venkateswara College of engineering and technology, Chittoor, A.P in 2018.