 ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print)

WSN Secure Coverage of Large Scale WSN Using Scalable Key Management Scheme

[1]Avala Venkata NookaRaju, [2]Renuka B, [3]Molli srinivasa Rao
[1,2,3]Dept of CSE, VITAM College of Engineering, Andhra Pradesh, India

Abstract
One of the foremost apprehensions when designing a key management scheme is the network scalability. Indeed the protocol should support a huge number of nodes to allow a large scale distribution of the network. An improved united-based key pre-distribution arrangement providing high network scalability and good key distribution probability approximately lower confined by $1 - e^{-1} \approx 0.632$. Results display that the proposed approach improves the network scalability while providing high secure connectivity coverage and complete better-quality performance. Furthermore, for an equivalent network size, our solution diminishes significantly the storage overhead compared to those of existing solutions.

Keywords
Wireless Sensor Networks, Security, Key Management, Network Scalability, Secure Connectivity Coverage

I. Introduction
A Wireless Sensor Network (WSN) contains of spatially distributed self-sufficient sensors to screen physical or environmental circumstances such as temperature, sound, pressure, etc. and to obligingly permit their data through the network to a main location. The recent networks are bi-directional, also empowering control of sensor activity. The expansion of wireless sensor networks was driven by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. The WSN is built of "nodes" from a few to numerous hundreds or even thousands, where each node is associated to one or occasionally several sensors. A sensor node might differ in size. The price of sensor nodes is similarly variable depending on the complexity of the individual sensor nodes.

II. Related Work
Key management problems in WSNs have been widely studied and numerous solutions have been proposed. In deterministic schemes, each two neighbouring nodes are able to inaugurate a through secure link which confirms a total secure connectivity coverage. In probabilistic schemes, the secure connectivity is not guaranteed because it is conditioned by the presence of shared keys between neighbouring nodes. In probabilistic key management schemes, each two neighbouring nodes can institute a secure link with some probability. If two neighbouring nodes cannot create a secure link, they create a secure path composed of consecutive secure links. Deterministic schemes confirm that each node is able to create a pair-wise key with all its neighbours.

III. Existing Method
Wireless Sensor Networks (WSNs) are progressively used in critical applications within several fields including military, medical and industrial sectors. Key management is a corner stone for numerous security services such as privacy and validation which are mandatory to secure communications in WSNs. The formation of secure links between nodes is then an interesting problem in WSNs. As of resource limitations, symmetric key formation is one of the most appropriate paradigms for securing interactions in WSNs. On the other hand absence of infrastructure in WSNs, we have usually no reliable third party which can feature pair wise secret keys to neighboring nodes, that is why most prevailing solutions are based on key pre-distribution.

IV. Disadvantages
A host of investigation effort dealt with symmetric key pre-distribution subject for WSNs and numerous answers have been suggested. In the existing system many disadvantages occur. The strategy of key rings as blocks of keys is strongly connected to the network size, these solutions either agonize from low scalability as number of supported nodes or reduce other presentation metrics including secure connectivity, storage overhead and resiliency in the case of huge networks.

V. Proposed Method
The objective is to challenge the scalability subject without degrading the other network performance metrics. For this resolution, we aim the design of a structure which ensures a good secure coverage of large scale networks with a low key storage overhead and a good network resiliency. To this end, we make use, of the unital design theory for efficient WSN key pre-distribution.

VI. Advantages
Systematic analysis that it permits to attain high scalability. Proposed an improved unital built key pre-distribution system that preserves a good key sharing probability while augmenting the network scalability. We study and associate our new approach in contradiction of main existing schemes, with respect to altered criteria as storage overhead, energy consumption, network scalability, secure connectivity coverage, average secure path length and network resiliency.

System Architecture

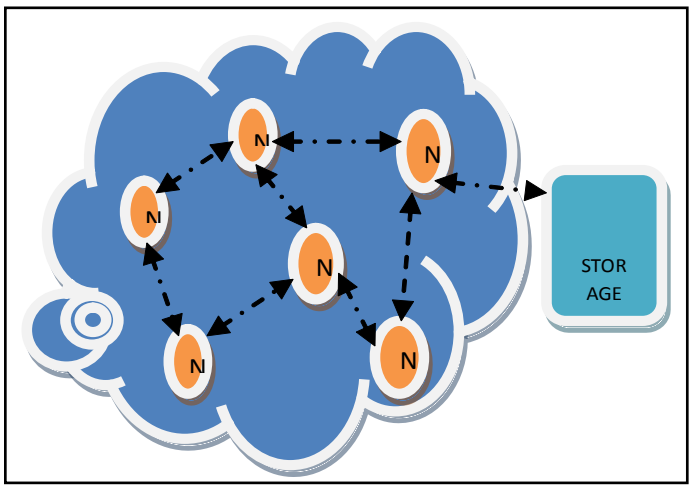

Fig. 1:

VI. Modules

A. Node Deployment

In the node deployment module where the node can be positioned by stipulating the number of nodes in the network. After specifying the number of nodes in the network, the nodes are positioned. The nodes are deployed with unique ID number so that each can be distinguished. And also nodes are deployed with their energy levels.

B. Key Generation

The key generation module is developed after node deployment module in which the number of nodes and number of blocks should be specified so that the key will be produced. The key is symmetric key and the key is displayed in the text area given in the node.

C. Key Pre-Distribution Technique

Generate blocks of m order primary design where every block resembles to a key set in this module. We pre-load then each node with t completely separate blocks where t is a protocol parameter. We validate the ailment of presence of such t completely separate blocks among the unital blocks. In the simple approach each node is pre-loaded with only single unital block and we proved that each two nodes share at most one key. Pre-loading every two nodes with t disjoint unital blocks resources that each two nodes share between zero and keys subsequently each two unitals blocks share at most single element. Later the deployment step, each two neighbors exchange the identifiers of their keys in order to regulate the common keys. This approach improves the network resiliency meanwhile the assailants have to cooperation more overlap keys to break a secure link. When neighbors do not segment any key, they should find a secure path collected of consecutive secure links.

D. Secure Transmission With Energy

The node distance is arranged and then the nodes with their neighbor information are demonstrated. So the nodes which is near by the node is selected and the energy level is first considered to confirm the secure communication. Later that the data is uploaded and directed to the destination node. Where in the destination node the key is verified and then the data is received.

VII. Results

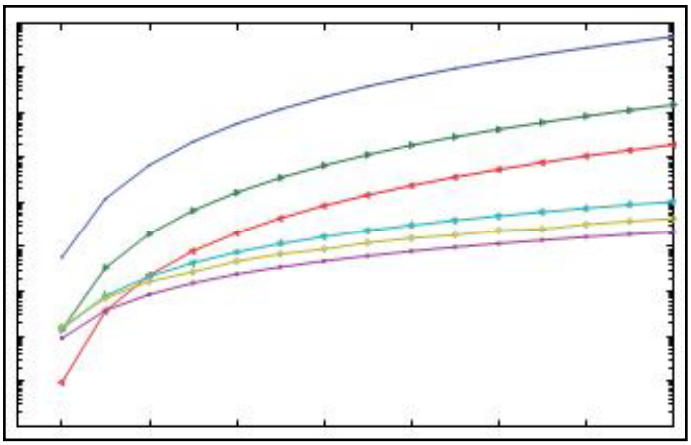

Fig. 2: Network Scalability at Equal Key Ring Size

We calculate for every network size the strategy order permit attaining the desired scalability and we presume then the key ring size, the attained results are reported in the figure. The fig. shows that at equal network size, the NU-KP system lets to decrease the key ring size and then the storage overhead. Though the value remains suggestively lower than the required key ring size of the SBIBD-KP. For illustration, the key ring size may be reduced over a factor greater than two when compared to the SBIBD-KP module.

VIII. Conclusion

A scalable key management arrangement which confirms a good secure coverage of large scale WSN with a low key storage overhead and a worthy network resiliency. We presented that a basic mapping from unitals to key pre-distribution let's to attain high network scalability while giving a low direct secure connectivity coverage. We planned then an effective scalable unital-based key pre-distribution system providing high network scalability and good secure connectivity coverage. We directed systematic analysis and simulations to associate our new solution to existing ones. The results presented confirms a high secure coverage of large scale networks while providing good overall performances.

References

[1] Y. Zhou, Y. Fang, Y. Zhang,"Securing wireless sensor networks: A Survey", IEEE Commun. Surv. Tuts., Vol. 10, No. 1–4, pp. 6–28, 2008.

[2] L. Eschenauer, V. D. Gligor,"A key-management scheme for Distributed sensor networks", In Proc. 2002 ACM CCS, pp. 41–47.

[3] H. Chan, A. Perrig, D. Song,"Random key predistribution schemes For sensor networks", In IEEE SP, pp. 197–213, 2003.

[4] W. Du, J. Deng, Y. Han, S. Chen, P. Varshney,"A key management Scheme for wireless sensor networks using deployment knowledge", In Proc. 2004 IEEE INFOCOM, pp. 586–597.

[5] C. Castelluccia, A. Spognardi,"A robust key pre-distribution protocol For multi-phase wireless sensor networks", in Proc. 2007 IEEE Securecom, pp. 351–360.

[6] D. Liu, P. Ning,"Establishing pairwise keys in distributed sensor Networks", In Proc. 2003 ACM CCS, pp. 52–61.

[7] Z. Yu, Y. Guan,"A robust group-based key management scheme for Wireless sensor networks", In Proc. 2005 IEEE WCNC, pp. 1915–1920.

[8] S. Ruj, A. Nayak, I. Stojmenovic,"Fully secure pairwise and Triple key distribution in wireless sensor networks using combinatorial Designs", In Proc. 2011 IEEE INFOCOM, pp. 326–330.

[9] S. Zhu, S. Setia, S. Jajodia,"Leap: efficient security mechanisms For large-scale distributed sensor networks", In Proc. 2003 ACM CCS, pp. 62–72.

[10] S. A. C¸ amtepe, B. Yener,"Combinatorial design of key distribution Mechanisms for wireless sensor networks", IEEE/ACM Trans. Netw., Vol. 15, pp. 346–358, 2007.

[11] A. Perrig, R. Szewczyk, V. Wen, D. E. Culler, J. D. Tygar, "Spins: Security protocols for sensor netowrks", In Proc. 2001 ACM MOBICOM, Pp. 189–199.

[12] B. Maala, Y. Challal, A. Bouabdallah,"Hero: hierarchcal key Management protocol for heterogeneous WSN", In Proc. 2008 IFIP WSAN, pp. 125–136.

[13] W. Bechkit, Y. Challal, A. Bouabdallah,"A new scalable key predistribution Scheme for WSN", In Proc. 2012 IEEE ICCCN, pp. 1–7.

[14] J. Zhang, V. Varadharajan,"Wireless sensor network key management Survey and taxonomy", J. Netw. Comput. Appl., Vol. 33, No. 2, pp. 63–75, 2010.
[15] S. A. C¸ amtepe, B. Yener,"Key distribution mechanisms for wireless Sensor networks: a survey", Technical Report TR-05-07, Mar. 2005.

Avala Venkata NookaRaju is pursuing his M.Tech in Computer Science and Engineering from VITAM College of Engineering affiliated to JNTU Kakinada. He received his M.Sc(Computer Science) degree from Spaces Degree College affiliated to Andhra University Visakhapatnam, Andhra Pradesh, India. His research interests include computer and network security.

Renuka B. She received her M.Tech in Computer Science and Technology from Andhra University, Visakhapatnam in 2010. She received her B.Tech from St.Theressa College of Engineering. She is currently working as Assistant Professor, CSE Dept. in VITAM College of Engineering, Andhra Pradesh, India. Her research interests include Computer Network Architectures, Algorithms and Protocols, Sensor Networks, Mobile Ad-hoc Networks, Wireless Mesh Networks, Computer and network security.

Molli srinivasa Rao is pursuing his Ph.D. from Andhra University. He received his M.Tech in Computer Science and Technology from Andhra University in 2003.He received his B.Tech degree from C.B.I.T., Hyderabad in 2001. He is currently working as Associate Professor, CSE Dept. in VITAM College of Engineering, Andhra Pradesh, India. His Research Interests include mobile Ad-Hoc Networks, Sensor Networks, Wireless Mesh Networks, Computer and network security.