ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 4, pp: (355-359), Month: October - December 2015, Available at: www.researchpublish.com

Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks

Syamsundar Guntur

Abstract: **Secure data transmission is a critical issue for wireless sensor networks (WSNs). Clustering is an effective and practical way to enhance the system performance of WSNs. In this paper, we study a secure data transmission for cluster-based WSNs (CWSNs), where the clusters are formed dynamically and periodically. We propose two Secure and Efficient data Transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the Identity-Based digital Signature (IBS) scheme and the Identity-Based Online/Offline digital Signature (IBOOS) scheme, respectively. In SET-IBS, security relies on the hardness of the Diffie-Hellman problem in the pairing domain. SET-IBOOS further reduces the computational overhead for protocol security, which is crucial for WSNs, while its security relies on the hardness of the discrete logarithm problem. We show the feasibility of the SET-IBS and SET-IBOOS protocols with respect to the security requirements and security analysis against various attacks. The calculations and simulations are provided to illustrate the efficiency of the proposed protocols. The results show that, the proposed protocols have better performance than the existing secure protocols for CWSNs, in terms of security overhead and energy consumption.**

Keywords: **Data Transmission, cluster-based WSNs (CWSNs), SET-IBS and SET-IBOOS.**

1. EXISTING SYSTEM

- In this Existing System of wireless sensor network comprised of spatially distributed devices using wireless sensor nodes to monitor physical or environmental conditions, such as sound, temperature, and motion.
- The individual nodes are capable of sensing their environments, processing the information data locally, and sending data to one or more collection points in a WSN.
- Efficient data transmission is one of the most important issues for WSNs. Meanwhile, many WSNs are deployed in harsh, neglected and often adversarial physical environments for certain applications, such as military domains and sensing tasks with trustless surroundings.

Existing System Algorithms:

- Sec LEACH Protocol
- LEACH Protocol.

Existing System Disadvantages:

- 1) The Communication speed will be very high.
- 2) There is no fixed routing path with less energy consumption.
- 3) The routing technique is flooding.
- 4) With respect to both computation and communication costs using Sec-LEACH and LEACH with high auxiliary security overhead is preferred for less secure data transmission in CWSNs.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 4, pp: (355-359), Month: October - December 2015, Available at: www.researchpublish.com

2. PROPOSED SYSTEM

- In this Proposed System, Secure and efficient data transmission is thus especially necessary and is demanded in many such practical WSNs.
- So, we propose two Secure and Efficient data Transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS
- It has been proposed in order to reduce the computation and storage costs to authenticate the encrypted sensed data, by applying digital signatures to message packets, which are efficient in communication and applying the key management for security.
- In the proposed protocols pairing parameters are distributed and preloaded in all sensor nodes by the BS initially.

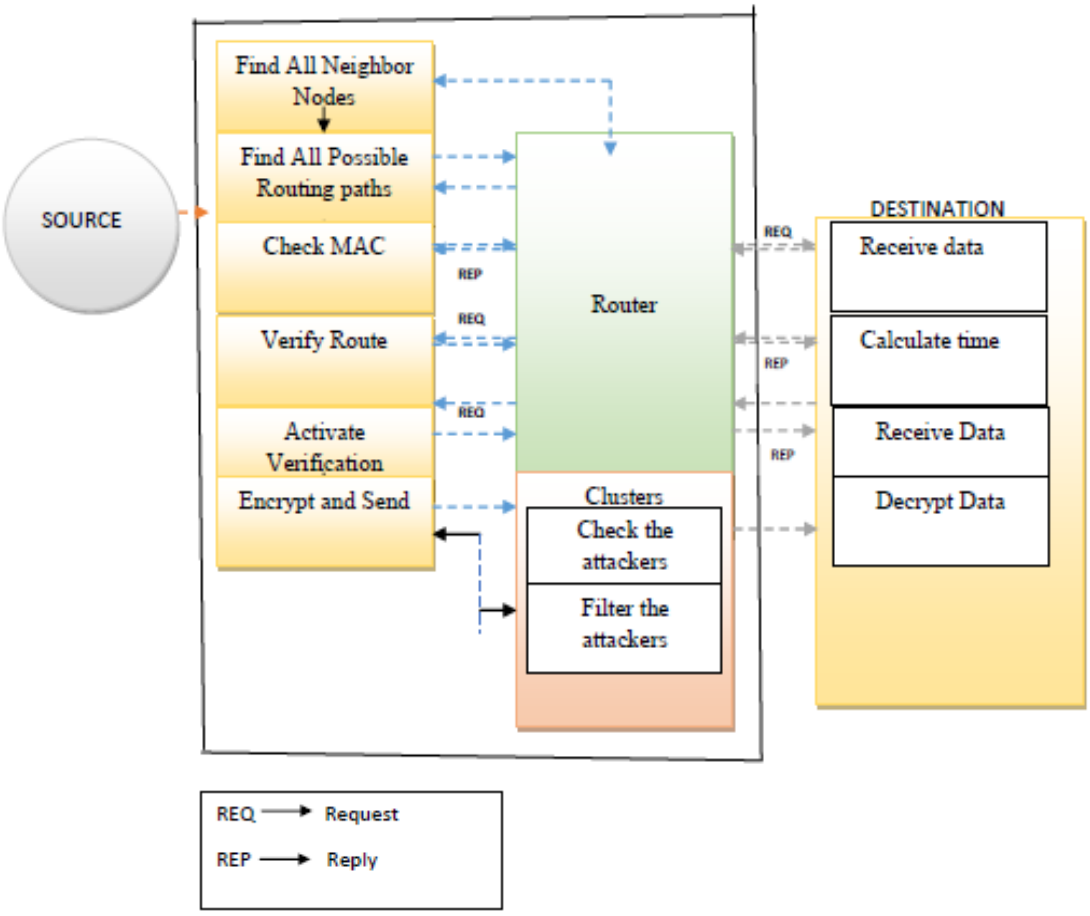
Proposed Algorithms:

- SET-IBS
- SET-IBOOS

ADVANTAGES OF PROPOSED SYSTEM:

- With respect to both computation and communication costs, we pointed out the merits that, using SET-IBOOS with less auxiliary security overhead is preferred for secure data transmission in CWSNs.
- The Nodes communications are very high using these protocols.
- The routing path is based on the Dijktra Algorithm where the communication links will take the less energy between the node

3. SYSTEM ARCHITECTURE



4. SYSTEM REQUIREMENTS

H/W SYSTEM CONFIGURATION:

- Processor : Pentium-IV
- Speed : 1.1GHz
- RAM : 512MB
- Hard Disk : 40GB
- General : Keyboard, Monitor, Mouse

S/W CONFIGURATION:-

- Operating System : Family (xp, win8, win7).
- Technologies : Java – AWT, Swings, Networking
- Software : JAVA (JDK 1.6.0)
- Protocol : TCP/IP
- IDE : Eclipse
- Data Base : MS Access / MY Sql

5. CONCLUSION

In this paper, we first reviewed the data transmission issues and the security issues in CWSNs. The deficiency of the symmetric key management for secure data transmission has been discussed. We then presented two secure and efficient data transmission protocols respectively for CWSNs, SET-IBS and SET-IBOOS. In the evaluation section, we provided feasibility of the proposed SET-IBS and SET-IBOOS with respect to the security requirements and analysis against routing attacks. SET-IBS and SET-IBOOS are efficient in communication and applying the ID-based crypto-system, which achieves security requirements in CWSNs, as well as solved the orphan node problem in the secure transmission protocols with the symmetric key management. Lastly, the comparison in the calculation and simulation results show that, the proposed SET-IBS and SET-IBOOS protocols have better performance than existing secure protocols for CWSNs. With respect to both computation and communication costs, we pointed out the merits that, using SET-IBOOS with less auxiliary security overhead is preferred for secure data transmission in CWSNs.

REFERENCES

[1] T. Hara, V. I. Zadorozhny, and E. Buchmann, Wireless Sensor Network Technologies for the Info. Explosion Era, Stud. Comput. Intell. Springer-Verlag, 2010, vol. 278.

[2] Y.Wang, G. Attebury, and B. Ramamurthy, “A Survey of Security Issues in Wireless Sensor Networks,” IEEE Commun. Surveys Tuts., vol. 8, no. 2, 2006.

[3] A. A. Abbasi and M. Younis, “A survey on clustering algorithms for wireless sensor networks,” Comput. Commun., vol. 30, no. 14-15, 2007.

[4] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “An application-specific protocol architecture for wireless microsensor networks,” IEEE Trans. Wireless Commun., vol. 1, no. 4, 2002.

[5] A. Manjeshwar, Q.-A.Zeng, and D. P. Agrawal, “An analytical model for information retrieval in wireless sensor networks using enhanced APTEEN protocol,” IEEE Trans. Parallel Distrib. Syst., vol. 13, 2002.

[6] S. Yi, J. Heo, Y. Cho et al., “PEACH: Power-efficient and adaptive clustering hierarchy protocol for WSNs,” Comput. Commun., vol. 30, no. 14-15, 2007.

[7] K. Pradeepa, W. R. Anne, and S. Duraisamy, “Design and Implementation Issues of Clustering in Wireless Sensor Networks,” Int. J. Comput. Applications, vol. 47, no. 11, 2012.

[8] L. B. Oliveira, A. Ferreira, M. A. Vilac¸a et al., "SecLEACH-On the security of clustered sensor networks," Signal Process., vol. 87, 2007.

[9] P. Banerjee, D. Jacobson, and S. Lahiri, "Security and performance analysis of a secure clustering protocol for sensor networks," in Proc. IEEE NCA, 2007.

[10] K. Zhang, C. Wang, and C. Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management," in Proc. WiCOM, 2008.

[11] S. Sharma and S. K. Jena, "A survey on secure hierarchical routing protocols in wireless sensor networks," in Proc. ICCCS, 2011.

[12] G. Gaubatz, J. P. Kaps, E. Ozturk et al., "State of the Art in Ultra-Low Power Public Key Cryptography for WSNs," in Proc. IEEE PerCom Workshops, 2005.

[13] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," in Lect. Notes. Comput. Sc. - CRYPTO, 2001.

[14] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," in Lect. Notes. Comput. Sc. - CRYPTO, 1985.

[15] D. W. Carman, "New Directions in Sensor Network Key Management," Int. J. Distrib. Sens. Netw., vol. 1, 2005.

[16] R. Yasmin, E. Ritter, and G. Wang, "An Authentication Framework for Wireless Sensor Networks using Identity-Based Signatures," in Proc. IEEE CIT, 2010.

[17] H. Lu, J. Li, and H. Kameda, "A Secure Routing Protocol for Cluster-Based WSNs Using ID-Based Digital Signature," in Proc. IEEE GLOBECOM, 2010.

[18] S. Even, O. Goldreich, and S. Micali, "On-Line/Off-Line Digital Signatures," in Lect. Notes. Comput. Sc. - CRYPTO, 1990.

[19] S. Xu, Y. Mu, and W. Susilo, "Online/Offline Signatures and Multisignatures for AODV and DSR Routing Security," in Lect. Notes. Comput. Sc. - Inf. Secur. Privacy, 2006.

[20] C.-K. Chu, J. K. Liu, J. Zhou et al., "Practical ID-based encryption for wireless sensor network," in Proc. ACM ASIACCS, 2010.

[21] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," Ad Hoc Networks, vol. 1, no. 2-3, 2003.

[22] F. Hess, "Efficient Identity Based Signature Schemes Based on Pairings," in Lect. Notes. Comput. Sc. - SAC, 2003.

[23] J. Liu and J. Zhou, "An Efficient Identity-Based Online/Offline Encryption Scheme," in Lect. Notes. Comput. Sc. - Appl. Crypto. Netw. Secur., 2009.

[24] J. J. Rotman, An Introduction to the Theory of Groups. Springer-Verlag; 4th edition, 1994.

[25] K. S. McCurley, "The discrete Logarithm Problem," in Proc. Symp. Appl. Math., Prog. Com. Sc., 1990, vol. 42.

[26] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Trans. Inf. Theory, vol. 22, no. 6, 1976.

[27] D. Boneh, I. Mironov, and V. Shoup, "A Secure Signature Scheme from Bilinear Maps," in Lect. Notes. Comput. Sc. - CT-RSA, 2003.

[28] P. Barreto, H. Kim, B. Lynn et al., "Efficient Algorithms for Pairing-Based Cryptosystems," in Lect. Notes. Comput. Sc. - CRYPTO, 2002.

[29] C. Castelluccia, E. Mykletun, and G. Tsudik, "Efficient aggregation of encrypted data in wireless sensor networks," in Proc. MobiQuitous, 2005.

[30] H. Lu, J. Li, and G. Wang, "A Novel Energy Efficient Routing Algorithm for Hierarchically Clustered Wireless Sensor Networks," in Proc. FCST, 2009.

[31] Y. Jia, L. Zhao, and B. Ma, "A Hierarchical Clustering-based Routing Protocol for WSNs Supporting Multiple Data Aggregation Qualities," IEEE Trans. Parallel Distrib. Syst., vol. 4, no. 1-2, 2008.

[32] "OMNeT++ Simulation Source Code." URL: http://www.osdp.cs.tsukuba.ac.jp/ luhuang/SCBRISS-sourcecode.rar

[33] B. Sun, L. Osborne, Y. Xiao et al., "Intrusion Detection Techniques in Mobile Ad Hoc and Wireless Sensor Networks," IEEE Wirel. Commun., vol. 14, no. 5, 2007.

[34] Secure Hash Standard, National Institute of Standards and Technology (NIST), Fed. Inf. Process. Stand. Publ. 180-1, 1995.

[35] D. Hankerson, S. Vanstone, and A. Menezes, Guide to Elliptic Curve Cryptography, Springer Prof. Comput. Springer, 2004.

[36] D. Liu and P. Ning, "Multilevel μTESLA: Broadcast authentication for distributed sensor networks," ACM Trans. Embed. Comput. Syst., vol. 3, 2004.

[37] "Crossbow Stargate," Crossbow Technology. URL: http://bullseye.xbow.com:81/ Products/productdetails.aspx?sid=229