International Journal On Engineering Technology and Sciences – IJETS™
ISSN (P): 2349-3968, ISSN (O): 2349-3976
Volume 1 Issue 6, October 2014

Efficient Anonymous Transfer of Data in Wireless Networks

K.HEMALATHA
M.E. CSE - FINAL YEAR
ASL PAULS COLLEGE OF ENGINEERING AND TECHNOLOGY, CBE.
hemalathakbe@gmail.com

Dr.*S.M.NANDHAGOPAL*
ASSOCIATE PROFESSOR, Department of Computer Science & Engineering,
ASL PAULS COLLEGE OF ENGINEERING AND TECHNOLOGY,CBE.
nandhagopalsm@gmail.com

Abstract— *We compare IBOOS with two recently proposed anonymous geographic routing protocols: AO2P and IBS which are based on hop-by-hop encryption and redundant traffic, respectively. All of the protocols are geographic routing, so we also compare IBOOS with the baseline routing protocol GPSR in the experiments. In GPSR, a packet is always forwarded to the node nearest to the destination. When such a node does not exist, GPSR uses perimeter forwarding to find the hop that is the closest to the destination. In IBS, each node periodically disseminates its own identity to its authenticated neighbors and continuously collects all other nodes' identities. Thus, nodes can build a secure map of other nodes for geographical routing. In routing, each node encrypts the packet by its key which is verified by the next hop en route. Such dissemination period was set to 30 s in this experiment.*

Key Words — GPSR, IBOOS, LEACH, Routing, Wireless networks.

I. INTRODUCTION

The goal of the proposed secure data transmission for CWSNs is to guarantee the secure and efficient data transmissions between leaf nodes and CHs, as well as transmission between CHs and the BS. In this paper, we aim to solve this orphan node problem by using the ID based cryptosystem that guarantees security requirements, and propose SET-IBS by using the IBS scheme. Furthermore, SET-IBOOS is proposed to reduce the computational overhead in SET-IBS with the IBOOS scheme.

There are some secure data transmission protocols based on LEACH-like protocols, such as Sec LEACH, GS-LEACH, and RLEACH. Most of them, however, apply the symmetric key management for security, which suffers from a so-called orphan node problem. This problem occurs when a node does not share a pair wise key with others in its preloaded key ring. To mitigate the storage cost of symmetric keys, the key ring in a node is not sufficient for it to share pair wise symmetric keys with all of the nodes in a network. In such a case, it cannot participate in any cluster, and therefore, has to select itself as a CH. Furthermore, the orphan node problem reduces the possibility of a node joining with a CH, when the number of alive nodes owning pairwise keys decreases after a long-term operation of the network. Since the more CHs elected by them, the more overall energy consumed of the network, the orphan node problem increases the overhead of transmission and system energy consumption by raising the number of CHs. Even in the case that a sensor node does share a pairwise key with a distant CH but not a nearby CH, it requires comparatively high energy to transmit data to the distant CH. The feasibility of the asymmetric key management has been shown in WSNs recently, which compensates the shortage from applying the symmetric key management for security. Digital signature is one of the most critical security services offered by cryptography in asymmetric key management systems, where the binding between the public key and the identification of the signer is obtained via a digital certificate. The identity-based digital signature (IBS) scheme, based on the difficulty of factoring integers from identity-based cryptography (IBC), is to derive an entity's public key from its identity information, for example, from its name or ID number. Recently, the concept of IBS has been developed as a key management in WSNs for security. Carman first combined the benefits of IBS and key predistribution set into WSNs, and some papers appeared in recent years. The IBOOS scheme has been proposed to reduce the computation and storage costs of signature processing. A general method for constructing online/offline signature schemes was introduced by Even et al. The IBOOS scheme could be effective for the key management in WSNs. Specifically; the offline phase can be executed on a sensor node or at the BS prior to communication, while the online phase is to be executed during communication.

- *K. Hemalatha is currently pursuing masters degree program in computer science engineering in ASL Pauls college of engineering and technology, Coimbatore, India. E-mail: hemalathakbe@gmail.com*
- *Dr.S. M. Nandhagopal M.E., Ph.D., is currently Head, Department of computer science & Engineering in ASL Pauls college of engineering and technology, Coimbatore, India. E-mail: nandhagopalsm@gmail.com*

II. RELATED WORKS

A. Routing Protocols

Hierarchical or cluster-based routing, originally proposed for wired network to enhance scalability and efficiency. In WSNs, Hierarchical routing techniques is used to enhance energy-efficiency and hence prolong the network lifetime. Reservation-based scheduling, collision avoidance, data aggregation by cluster head, uniform energy dissipation, fair allocation of channel and lower latency are some characteristics of hierarchical topology routing protocol. Low energy adaptive clustering hierarchy is one of the very first hierarchical routing protocols. LEACH includes distributed clustering and utilizes randomize rotation of cluster heads to evenly distribute the energy load in the network. It calculates a threshold value to elect the cluster head. LEACH protocol is very useful for the applications, where constant monitoring is required. TL-LEACHis the extension of the LEACH, where TL stands for two-Level. It utilizes two level of clustering where primary CH communicate with secondary CH in order to send the data, for better throughput. TL-LEACH form clusters based on minimum distance of nodes to their corresponding CH, EECS extends this by dynamic sizing of clusters based on cluster distance from the base station. CH election is based on the residual energy of the node.

Power-efficient gathering in Sensor Information System (PEGASIS) is a near-optimal chain-based protocol. In PEGASIS, nodes need to communicate to its nearest neighbor and they propagate to the base-station. Unlike LEACH, PEGASIS avoids cluster formation and uses only one node in a chain to transmit to the base-station. In this way it increase the lifetime of the network and allow only local communication for less bandwidth consumption in communication. Further reduce the energy consumption of PEGASIS, CCS has been proposed. In CCS, the whole network is divided in co-centric circular tracks and each track presents a cluster. Track level has been assign to each track, depends upon the distance from the base-station. Data communication is done through tracks. TSC protocol is the enhance version of CCS, by further dividing tracks into sectors.

B. Attacks on Routing Protocol

Many sensor network routing protocols were very simple and not developed as security in mind, so the adversary can launch various attacks in the network. Mainly network layer protocol (i.e. routing protocol) suffers from many attacks like; spoofing or altering the route information, selective forwarding, sinkhole attack, wormhole attack, Sybil attack, etc.

C. Spoofing, Altering Or Replaying The Route Information

An adversary can launch the routing information corruption by spoofing, altering or replying the routing information. By this an adversary can attracts or redirects the traffic, increases the latency, generate routing loops or creates false error etc.

D. Selective forwarding attack

In the selective forwarding attack, malicious node may refuse to forward certain packet and simply drop it. If an adversary drops the entire received packet, it behaves like a blackhole attack. An adversary explicitly includes on the path of data flow to perform selective forwarding.

E. Sinkhole and Wormhole attack

Basically, in the both sinkhole and wormhole attacks; the adversary tries to attract all the traffic from a particular area through a compromised node. Sinkhole attack mainly works by making a compromised node look attractive to the neighbor nodes to route the data packet and generally spoof, modify or drop the packet. In this way, sinkhole attack give birth to many attacks like; selective forwarding, blackhole, tempering the routing information etc. An adversary launch wormhole with two distant malicious nodes and try to attract the traffic by showing one hop distance to the sink. Wormhole attack is very difficult to detect because it uses out-of-bound channel to route packets.

F. Sybil attack

In this attack a single node presents multiple identities to the other node in the network. It tries to mislead the node in neighbor detection, route formation and topology maintenance. The Sybil attack is a significant threat to many geographic and multipath routing protocols.

III. OUR WORK

Many previous Hierarchical routing protocols assume a safe and secure environment where all sensor nodes cooperate with no attack present. But the real world environment is totally opposite, there are many attacks that affects the performance of routing protocol. Attacker use different kinds of technique to launch attack and damage or harm the data and the network. In order to secure the hierarchical routing protocol many works have been proposed. In this section we discuss those techniques, analyze them and list out the advantages and disadvantages associated with each secure hierarchical routing protocol.

A. Sec-LEACH

Sec-LEACH provides an efficient solution for securing communications in LEACH. It used random-key predistribution and μTESLA for secure hierarchical WSN with dynamic cluster formation. Sec-LEACH applied random key distribution to LEACH, and introduced symmetric key and one way hash chain to provide confidentiality and freshness. Sec-LEACH provides authenticity, integrity, confidentiality and freshness to communications.

B. SS-LEACH

A secure hierarchical protocol called SS-LEACH, which is the secure version of LEACH. SSLEACH improves the method of electing cluster heads and forms dynamic stochastic multi-paths cluster heads chains to communicate to the base station, In this way it improve

IJETS

the energy-efficiency and hence prolong the lifetime of the network. It used the key pre-distribution and self-localization technique to secure the basic LEACH protocol. It prevent compromised node to take part in the network and preserve the secrecy of the packet. It avoids selective forwarding, HELLO flooding and Sybil attack.

C. *ID-based Online/Offline Signature (IBOOS)*

An Online/Offline Signature (OOS) scheme divides the process of message signing into two phases, the Offline phase and the online phase. The Offline phase is performed before the message to be signed becomes available. This phase performs most of the computations of signature generation and results in a partial signature. Once the message is known, the Online phase starts. This phase retrieves the partial signature calculated during the Offline phase and performs some minor quick computations to obtain the final signature. The Online phase is assumed to be very fast, consisting of small computations while the Offline phase can be performed by any other resourceful device. IBOOS is the ID-based version of OOS, where a message signed with a signer's private key is verified using the signer's ID. In ID-based cryptography, the signer's private key corresponding to his ID is generated by a private key generator (PKG). IBOOS enables a resource constrained sensor node to sign a message quickly, once it has some critical event to report. Moreover, some IBOOS schemes, allow reusing the partial signature computed in the offline phase to sign more than one message, which decreases the energy consumption on sensor nodes.

IV. IMPLEMENTATION AND EVALUATION

A. *Choice of IBOOS Schemes*

There are many IBOOS schemes available, for example, based on Elliptic Curve Cryptography (ECC) and RSA signatures. Keeping in mind the security and efficiency requirements, the two different ECC based IBOOS schemes given were selected for implementation and evaluation purposes. The IBOOS scheme proposed to presents a method to convert an underlying signature scheme into an online/offline signature scheme to mitigate phishing attacks. The offline signature in this scheme can be securely reused to sign more than one message. This signature scheme is proved to be existentially unforgeable. Its security depends on the Discrete Logarithm Problem. Unlike R-IBOOS, the IBOOS scheme presented. It provides a direct online/ offline signature scheme for authentication in mobile ad-hoc networks, which does not require another underlying signature scheme. This signature scheme is existentially unforgeable under adaptive chosen message attacks. To see how efficient these IBOOS schemes would be on sensor nodes, we went for the implementation of these IBOOS schemes on actual sensor nodes. However, we only implemented X-IBOOS scheme and based on the implementation results, we decided to skip RIBOOS.

V. DISCUSSION

Our implementation results obtained in Sec. 4 strengthened the idea of using online/offline signatures for resource constrained sensor nodes. The X-IBOOS scheme proved expensive for the sensor nodes, consuming considerable resources. The reason behind this was not the online/offline signature itself but the expensive pairing based cryptography. The implementation results of B-IBOOS proved this argument. Hence, if we use pairing-free ECC based IBOOS schemes we can obtain better results. Moreover, the two implementations of B-IBOOS offer a trade-off between the computation cost and the memory usage. Memory can be saved by removing the precomputed table and slightly increasing the computation time. However, this can be decided depending on the type of application.

The offline signature is computed before the message to be signed is available and the online phase takes the same time in both implementations, i.e., 0.025s. Therefore, the time to compute the final signature, once the message is known, is the same in both cases. For time critical applications, it is reasonable to use the first implementation of B-IBOOS if the receiver is a sensor node, and the second implementation of B-IBOOS if the receiver is a powerful device. Broadcast of a message by a sensor node is not a very frequent event in time critical applications, for instance, forest fire alarm application. In forest fire alarm application, a message is sent by a sensor node only when a fire is set up somewhere in the forest. Signing and verifying a message occasionally only in critical situations is not very expensive for the sensor nodes. Moreover, if the offline phase is performed on the base station and the resulting offline signature is stored on the sensor node, it can further reduce the computation overhead on the sensor nodes. X-IBOOS can also be useful for such applications of WSNs where the offline signature is computed and stored by the base station on the sensor nodes and the signature verifier is a powerful device.

VI. CONCLUSION

Routing protocol affects the performance of the network in the form of energy efficiency, security, resiliency and lifetime. So that secure, robust and efficient routing protocol is the basic requirement. In this paper, we have studied and analyzed a number of secure and energy efficient hierarchical routing protocols for WSN. The information provided in the paper would be beneficial for the researchers to work in this area.

We assessed the cost incurred by using two different IBOOS schemes for resource constrained sensor nodes. We first implemented and evaluated one pairing based IBOOS scheme named as XIBOOS. For optimization purposes, we also converted the well-known pairing-free BNN-IBS scheme into an IBOOS scheme and implemented it on MICA2 sensor nodes. The implementation results show the suitability of IBOOS for

IJETS

WSNs. In future, we are going to focus on the session key establishment between the outsider user and the sensor node after successful user authentication, i.e., the second authentication scheme of the proposed framework.

REFERENCES

[1] T. Hara, V.I. Zadorozhny, and E. Buchmann, "*Wireless Sensor Network Technologies for the Information Explosion Era*", Studies in Computational Intelligence, vol. 278. Springer-Verlag, 2010.

[2] Y. Wang, G. Attebury, and B. Ramamurthy, *"A Survey of Security Issues in Wireless Sensor Networks,"* IEEE Comm. Surveys & Tutorials, vol. 8, no. 2, pp. 2-23, Second Quarter 2006.

[3] A.A. Abbasi and M. Younis, *"A Survey on Clustering Algorithms for Wireless Sensor Networks",* Computer Comm., vol. 30, nos. 14/ 15, pp. 2826-2841, 2007.

[4] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, *"An Application-Specific Protocol Architecture for Wireless Microsensor Networks,"* IEEE Trans. Wireless Comm., vol. 1, no. 4, pp. 660- 670, Oct. 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 & Distributed Systems, vol. 13, no. 12, pp. 1290-1302, Dec. 2002.

[6] S. Yi et al., *"PEACH: Power-Efficient and Adaptive Clustering Hierarchy Protocol for Wireless Sensor Networks,"* Computer Comm., vol. 30, nos. 14/15, pp. 2842-2852, 2007.

[7] K. Pradeepa, W.R. Anne, and S. Duraisamy, *"Design and Implementation Issues of Clustering in Wireless Sensor Networks,"* Int'l J. Computer Applications, vol. 47, no. 11, pp. 23-28, 2012.

[8] L.B. Oliveira et al., *"SecLEACH-On the Security of Clustered Sensor Networks,"* Signal Processing, vol. 87, pp. 2882-2895, 2007.

[9] P. Banerjee, D. Jacobson, and S. Lahiri, *"Security and Performance Analysis of a Secure Clustering Protocol for Sensor Networks,"* Proc. IEEE Sixth Int'l Symp. Network Computing and Applications (NCA), pp. 145-152, 2007.

[10] K. Zhang, C. Wang, and C. Wang, *"A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management,"* Proc. Fourth Int'l Conf. Wireless Comm., Networking and Mobile Computing (WiCOM), pp. 1-5, 2008.

IJETS