IJCTA, 10(02), 2017, pp. 21-25

Security and Performance to Identifying Efficient Key Mangement in Wormhole Attack

M. Mythily* and S. Saravana Kumar**

Abstract : In this research paper, we propose An Efficient Group Key Management using Symmetric Key and Cryptography for Cluster based Wireless Sensor Networks (EGKMST). Based on hierarchical cluster structure of sensor network, the proposed scheme adopted the pair-wise key management and group key management based on threshold key cryptography to generate and to distribute the keys efficiently within a cluster and updates periodically keys. By this way, EGKMST scheme provides continuous transmission security and avoids dangerous attacks from malicious nodes and mitigate the node compromise attack in WSNs communication. Therefore we find that the communication overhead which EGKMST protocol leads is negligible for keys establishment with low memory overhead and energy savings. The proposed scheme provides better connectivity and scalability with few messages than previous schemes based on deterministic approach and schemes based on random key pre-distribution schemes based on key pools which generate a lot of message with high storage overhead. Security and performance analysis have shown that EGKMST approach can not only provide energy savings that increase the network lifetime, but also can achieves efficient security with low key storage overhead.

Keywords: Wormhole, attack, wireless, host, packet, wireless.WSN.

1. INTRODUCTION

The methods proposed in the previous researches can be broadly explained. EGKMST provides basic security requirements and is secure against spoofed, altered and replayed packets attacks. In these attacks, adversary alters, spoof or replay the routing information [10]. It can also reply routing information. As a result, it could increase the delay. Further, before message transmission, encryption is performed to secure the communication with the help of one way hash function, used to provide authentication and message integrity. In EGKMST, each cluster members encrypts information using the intra-cluster pairwise key KCi-Si and the intra-cluster group key KGroup, avoiding eavesdropping attacks. Therefore only legitimate CH that owns KCi-Si key and KGroup can decrypt the message. EGKMST provides freshness using time interval, time-stamps and nonce. The nonce N is very important since it prevents a replay attack and ensures the integrity of the message. Further to know the origination of the message for further action, BS and nodes check the id which is attached to the message.

1.1. Techniques to Remove Wormhole Attack

1.1.1. Routing Leashes Algorithm

Routing attacks for single-path routing have been identified for wireless ad hoc networks and the corresponding counter measures have been proposed in the literature. However, the effects of routing

* Research scholars, Dept of Computer Science Engineering, Bharath University,Chennai

** Professor, Department of CSE, Karpagam College of Engineering, Coimbatore *saravanakumars81@gmail.com,shreemysur23@yahoo.com*

attacks on multi-path routing have not been addressed. In this paper, the performance of multi-path routing under wormhole attack is studied in detail. The results show that multi-path routing is vulnerable to wormhole attacks. A simple scheme based on statistical analysis (called SAM) is proposed to detect such attacks and to identify malicious nodes. Comparing to the previous approaches (for example, using packet leash), no special requirements (such as time synchronization or GPS) are needed in the proposed scheme. Simulation results demonstrate that SAM successfully detects wormhole attacks and locates the malicious nodes in networks with different topologies and with different node transmission range. Moreover, SAM may act as a module in local detection agents in an intrusion detection system (IDS) for wireless ad hoc networks..

In Temporal Leashes, all nodes are required to maintain a tightly synchronized clock but do not rely on GPS information. When temporal leashes are used, the sending node append the time of transmission to each sent packet *ts* in a packet leash, and the receiving node uses its own packet reception time *tr* for verification. The sending node calculates an expiration time *te* after which a packet should not be accepted, and puts that information in the leash. To prevent a packet from travelling farther than distance L, the expiration time is set to:

$$te = ts + (L/c) - \Delta$$

Where c is the speed of light and Δ is the maximum clock synchronization error. All sending nodes append the time of transmission to each sent packet. The receiver compares the time to its locally maintained time and assuming that the transmission propagation speed is equal to the speed of light, computes the distance to the sender. The receiver is thus able to detect, whether the packet has travelled on additional number of hops before reaching the receiver. Both types ofleashes require that all nodes can obtain an authenticated symmetric key of every other node in the network. These keys enable a receiver to authenticate the location and time information in a received packet.

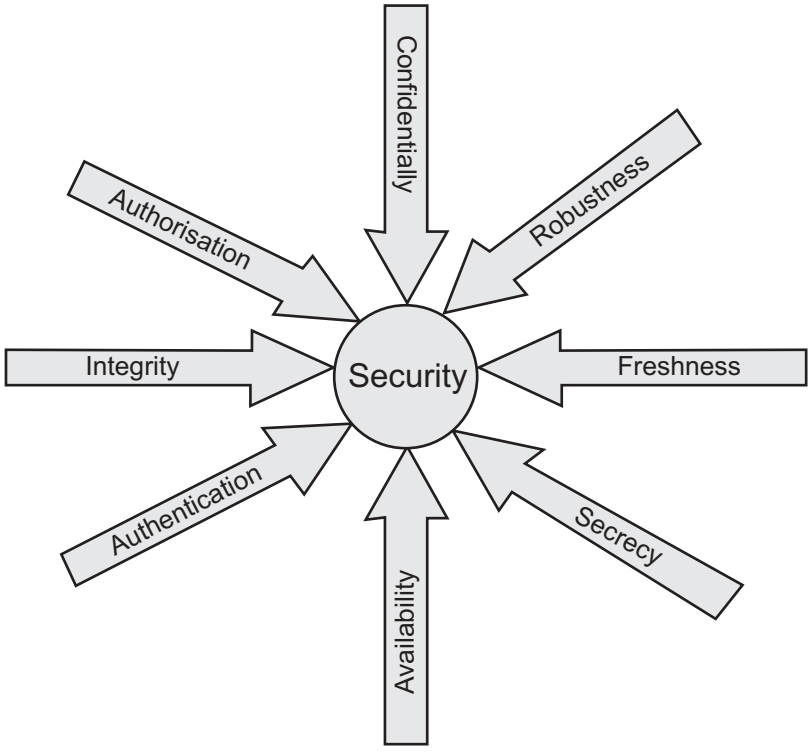

Figure 1

An Efficient Group Key Management using Symmetric Key and Threshold Cryptography for Cluster based Wireless Sensor Networks (EGKMST). The proposed scheme considers a hierarchical cluster structure of sensor network [11]. EGKMST adopts pair-wise key management and group key management based on threshold key cryptography [12, 13] to generate and to distribute the keys efficiently within a cluster and updates periodically keys. By this way EGKMST provides continuous transmission security

1.1.2. State Routing

State routingis a routing protocol which routes the data using the location of the nodes. In this paper [1,5] we present the possible attacks on BSR protocol. These attacks are difficult to be detected. To avoid the attacks on BSR protocol, we propose two schemes namely Reverse Routing Scheme (RRS) and Authentication of Nodes Scheme (ANS).

To detect and thus defend against wormhole attacks. In this attack, an attacker records a packet or individual bits from a packet, at one location in the network, tunnels the packet (possibly selectively) to another location, and replays it there.

Geographic routing protocols use a basic geographic forwarding strategy to forward packets node by node toward the location of the destination. This approach to routing has the advantage of eliminating the need for nodes to maintain conventional routing information.

The routing protocol must deal with threats from external agents and compromised internal nodes. The lack of a central control and the fact that each node must forward packets of other nodes represent major security challenges. In such environments it is difficult to assure the confidentiality and the integrity of the communications as well as the availability of the services.

1.1.2.1. On Asymmetric Cryptographic Techniques

PKI Interaction : An (offline) PKI Authority is in charge of certifying or assigning keys of each node participating in the trusted network. Each node joining the network will have the public key of of the certification authority, as pictured on figure 1. This key is denoted the *global key*.

Key Distribution : Later, any node entering the ad-hocnetwork could diffuse its public keys, with a specific key exchange protocol, as pictured on figure 9, with proper parameters,certificates and signatures. The key which is used

later to sign message is denoted the *local key*, and can be either its global key, or newly generated private/public keys.

Protocol Message Signing : At the same time, the node would start originating OLSR control messages, signing them using the local key with a specific extension which prepends a special signature message.

2. CONCLUSION

In order to give more robust protection in some special scenario, where highly secured information is required there is a need of developing some secured.We examine the security issues, and describe an architecture including multiple securing mechanisms. The attacks prevented by this architecture, along with details about protocols, algorithms, mechanisms and implementation details are given.

The main objectives of this approach are To prevent eavesdropping, avoid packet modification and provide authentication & confidentiality. To reduce the packet overhead.The proposed solution unlike some of its predecessors does not require any specialized hardware like directional antennas, etc for detecting the attackers. or extremely accurate clocks, etc. Currently more studies are being done to analyze the performance of the proposed algorithm in presence of multiple attacker node. Our future works may concentrate to develop and implement in the real environment a complete security protocol with low storage and energy savings.

3. REFERENCES

1. Wormhole Attacks in Wireless NetworksYih-Chun Hu, Member, IEEE, Adrian Perrig, Member, IEEE, and David B. Johnson, Member, IEEE IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO. 2, FEBRUARY 2006
2. IN THE PAPER Detection and Prevention of Layer-3 Wormhole Attacks on Boundary State Routing in Ad hoc Networks.2010 International Conference on Advances in Computer Engineering

3. Y.C. Hu A. Perrig and D. B. Johnson. PACKET LEASHES: A defense against wormhole attacks in wireless ad hoc networks. IEEE INFOCOM, pages 1976–1986, 2003. 612–621, 2005
4. H.S. Chiu and K.S. Lui. DELPHI: wormhole detection mechanism for ad hoc wireless networks. 1st International Symposium on WirelessPervasive Computing, pages 6–11, January 2006.
5. Ming-Yang Su. Warp: A wormhole-avoidance routing protocol by anamoly detection in mobile ad hoc networks. Computer Security, vol.29, March 2010.
6. S Dharmaraja and Subrat kar:WHOP: Wormhole Attack Detection Protocol using Hound Packet. 2011 international conferenceon innovation in information technology
7. On the Survivability of Routing Protocols in Ad Hoc Wireless Networks, A. Baruch, R. Curmola, C. Nita-Rotaru, D. Holmer, H. Rubens, Converence onSecurity and Privacy for Emerging Areas Communications, SecureComm 2005, September2005.
8. I. Khalil S. Bagchi and N.B. Shroff. LITEWORP: a lightweightcounter measure for the wormhole attack in multihop wireless networks.International Conference on Dependable Systems and Networks, pages 612–621, 2005.
9. Issa Khalil, Saurabh Bagchi & Ness B. Shroff, “MOBIWORP: Mitigation of the Wormhole Attack in Mobile Multihop Wireless Networks”. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4198824
10. A Survey on Complex Wormhole Attack in Wireless Ad Hoc Networks 2009 International Conference on Advances in Computing, Control, and Telecommunication Technologies.1
11. C K Toh, Ad Hoc Mobile Wireless Networks, Prentice Hall Publishers , 2002.
12. P. Gupta and P.R. Kumar. Capacity of wireless networks. IEEE Transactions on Information Theory, Volume 46, Issue 2, March 2000, doi:10.1109/18.82579.
13. Jinyang Li, Charles Blake, Douglas S. J. De Couto, Hu Imm Lee, and Robert Morris, Capacity of Ad Hoc Wireless Networks, in the proceedings of the 7th ACM International Conference on Mobile Computing and Networking, Rome, Italy, July 2001.
14. Wu S.L., Tseng Y.C., “Wireless Ad Hoc Networking, Auerbach Publications”, 2007 ISBN 978-0-8493-9254-2.
15. Tomas Krag and Sebastian Büettrich (2004-01-24). “WirelessMesh Networking”. O’Reilly Wireless Dev Center. Retrieved 2009-01-20.
16. Y.-C. Hu, A. Perrig, D. B. Johnson, “Wormhole Attacks in Wireless Networks,” Selected Areas of Communications, IEEE Journal on, vol. 24, numb. 2,pp. 370- 380, 2006.
17. Y. Hu, A. Perrig, and D. Johnson, “Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks”, in proceedings of INFOCOM, 2004.
18. W. Weichao, B. Bharat, Y. Lu, X. Wu, Wiley Interscience, “Defending agains Wormhole Attacks in Mobile Ad Hoc Networks,” Wireless Communication and Mobile Computing, January 2006.
19. M.A. Azer S.M. El-Kassas A. Wahab F Magdy S and El-Soundani. Intrusion detection for wormhole attacks in ad hoc networks a survey and a proposed decentralized scheme. In the proceedings of the IEEE international conference on availability, reliability and security, pages 630–646, 2008.
20. G. Lee D. Kim and J. Seo. An approach to mitigate wormhole attack in wireless ad hoc networks. In the proceedings of the internationalconference on information security and assurance, pages 220–225, 2008.
21. Ming-Yang Su. Warp: A wormhole-avoidance routing protocol by anamoly detection in mobile ad hoc networks. Computer Security, vol. 29, March 2010.
22. Y.C. Hu A. Perrig and D. B. Johnson. PACKET LEASHES: A defense against wormhole attacks in wireless ad hoc networks. IEEE INFOCOM, pages 19
23. Security Lab in the Computer Science Department at Stanford University, ibe-0.7.2.tgz implementation of Identity-Based Encryption (and signature), http://crypto.stanford.edu/ibe/.
24. J.H Cheon, Y.D. Kim, H.J. Yoon “A New ID-based Signature with Batch- Verification”, Cryptology ePrint Archive, Report 2004/131.
25. W. Dai et al., “Crypto++”, http://www.eskimo.com/˜weidai/cryptlib.html
26. M. Scott, MIRACL, Multiprecision Integer and Rational Arithmetic C/C++ Library, http://indigo.ie/˜mscott/

27. S. Galbraith, K. Harrison, D. Soldera, “Implementing the Tate pairing”, HP Laboratories Research Report HPL-2002-23, March 2002.

28. P.S.L.M. Barreto, H.Y. Kim, B. Lynn, M. Scott, “Efficient Algorithms for Pairing-Based Cryptosystems”, Crypty’2000, LNCS 2442, pp 354–368.

29. Jorji Nonaka, Gerson H. Pfitscher, Katsumi Onisi, Hideo Nakano “An Evaluation of Low Cost Hardware-assisted Internal Clock Synchronization in PC Cluster Environment”, PDPTA 2002, pp 456-461.

30. J. R. Vig, “Introduction to Quartz Frequency Standards”, SLCETTR - 92-1 (rev. 1), Army Research Laboratory, Electronic and Power Sources Directorate, Fort Monmouth, NJ, October 1992.

31. The IEEE P1363 Working Group, Standard Specifications For Public- Key Cryptography.

32. Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks. In Proceedings of the 8th ACM International Conference on Mobile Computing and Networking, September 2002.