Enhanced Technique for Secure Wireless Sensor Routing with Respect to Energy Conservation

Maqsood Mahmud[1,3,4], Abdulrahman Abdulkarim Mirza[1,4], Ihsan Ullah[2],
Naveed Khan[2], Abdul Hanan Bin Abdullah[3], and Mohammad Yazid Bin Idris[3]

[1] Department of Information System
[2] Department of Computer Science,
College of Computer and Information Sciences
King Saud University, Saudi Arabia
[3] Faculty of Computer Science and Information Systems,
Universiti Teknologi Malaysia, Malaysia
[4] Center of Excellence in Information Assurance (CoEIA),
King Saud University, Saudi Arabia
{maqsood.m,amirza,ihsanullah,naveed}@ksu.edu.sa,
{hanan,yazid}@utm.my

Abstract. This paper presents a routing protocol architecture based on recursive group algorithm. This algorithm apply Group Verification Tree approach which makes the sensor network secure and make it safer from malicious intrusions and illegitimate users. The proposed approach will give a new dimension to the fast and secure routing in the sensor networks with less energy to be consumed. Based on the analysis and simulation the proposed strategies yield better results than the existing results.

Keywords: Group Verification Tree, Malicious, Routing Protocol, Wireless Sensor Networks.

1 Introduction

Our introduction is based on the following measurements and concepts.

1.1 Sample Attacks on Routing

The following attacks are brought into account while studying the above algorithm [5][9]. Inject incorrect routing information or alter setup/update messages like Compromised sensors are most problematic. It provides malicious routing data/messages suppress (selectively) routing messages. Specific attacks are Black hole, Wormhole, Replication and Denial of Service.

1.2 Techniques for Secure Routing

The basic three techniques that we are using for secure routing are Prevention, Detection & Recovery and Resilience [3] which uses certain techniques discussed later.

T.-h. Kim et al. (Eds.): FGIT 2010, LNCS 6485, pp. 376–382, 2010.

2 Related Work

The Sensor routing is the most assumed trusted environment. INSENS is only applicable to certain topologies. SIGF requires GPS and Other secure routing protocols [7]. It typically relies on a single technique. For Prevention it uses S-BGP, Ariadne. For Detection & Recovery it uses Watchdog, Pathrater, and Secure Traceroute. While Resilience uses INSENS[8]. The inappropriate resource-constrained sensor nodes require PKI or excessive amounts of memory, computation or communication [13]. Wireless Sensor Networks technology becomes progressively more valuable in public safety, home, medical and office security as well as in military security. Secure-SPIN implements in wireless sensor Networks has three phases using of PASC protocol for confidentiality, eliminating of malicious user through Hash function and in energy conservation through CDMA code [1]. Energy consumption is a key measure in sensor Networks. The multiple node-disjoints paths can be discovered through distributed multi path routing protocol and energy a wearing routing protocols. The load balancing algorithm is used to distribute traffic over multiple paths [2].

3 Routing Protocol Architecture Used

This paper establishes routing tables and network addresses using prevention techniques to thwart active attackers. To detect and recover from attempts to deviate from the protocol or to launch additional attacks and apply resilient routing techniques to forward packets. It uses the securely established routing tables and network addresses [1].

3.1 Our Assumptions

Our assumptions are Network authority (NA) uses a public/private key pair {K_{NA}, K^{-1}_{NA}}, each sensor node preloaded with, Network authority's public key K_{NA} ,Unique $ID_{x,}$ Certificate: Sig(K^{-1}_{NA}, ID_x), Signature scheme optimizes for verification, Intended for networks of primarily stationary sensors.

3.2 Address and Route Setup

Goal assigns a unique network address to each node to populate each node's routing table to accomplished with a recursive grouping algorithm, initially, each sensor constitutes its own group, groups repeatedly merge until all nodes belong to same group. Each time a node's group merges, the node adds one bit to its network address and one entry to its routing table.

3.3 Recursive Grouping Algorithm

In this scenario each Group act in an asynchronous, distributed fashion and is explained below categorically [12]. Each group collects information about its neighbors, proposes to merge with smallest neighboring group. It is based on number of nodes in the group, ties broken based on group ID. This metric keeps addresses and routing tables small. The mutual proposal triggers merge entire process is deterministic for a given topology. It limits the damage. An attacker can inflict.

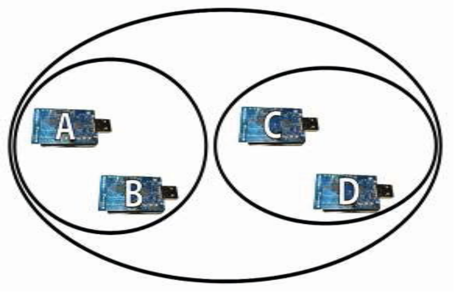

Fig. 1. Initial Convergence

Table 1. Detecting Grouping Deviations

Node Id	Address	Routing Table
A	0.0	RT_A
B	0.1	RT_B
C	1.0	RT_C
D	1.1	RT_D

3.4 Calculating Network Addresses

Assume G and G' decide to merge each node in G independently extends its network address by one bit. It is based on Nodes in G' which make similar changes while merging.

$$R_i = \begin{cases} 0 & ID_G < ID_{G'} \\ 1 & ID_G > ID_{G'} \end{cases} \tag{1}$$

3.5 Populating Routing Tables

Let's assume G and G' decide to merge and each node in G records the neighbor from whom it heard about G' in its current routing table slot

3.6 Forwarding

In this method the basic forwarding is similar to area-style forwarding. If given a destination network address route towards node with longest matching prefix will be adopted. (i) Path length in logical hops bound by log (n), (ii) A logical hop may require several physical hops.

4 Threats

The compromised nodes may lie about group size or ID to subvert route setup and compromised nodes may claim multiple IDs or try to simultaneously group with several other nodes [2][9][10].

4.1 Detecting Grouping Deviations

To Maintain a Grouping Verification Tree (GVT) for each group during recursive grouping it prevents attacker from lying about group ID or size, based on a hash tree construction [6]. Before two groups merge, they verify each other's GVT. Integrity of the GVTs insures integrity of the recursive grouping algorithm. Final GVT covers all nodes in the network. It can be used to authenticate any node's network address to prevent illegal node to the sensor networks.

4.2 Hash Trees

We used Hash function which has O(1) time complexity. To employ a one-way hash function H: {0,1}*→{0,1}ρ has to be observed. To create a one-way data structure-the Merkle Tree is one such data structure that has to be used.

- Each internal node calculated as:
  Parent = H(ChildL || ChildR)
- Authenticates a leaf node given the root value and nodes along the path to the root

4.3 Group ID Computation

To assume G and G' decide to merge. Each node in G independently calculates the new group ID as:

$$ID_{\gamma} = \begin{cases} h(ID_G, |G|, ID_{G'}, |G'|) & ID_G < ID_{G'} \\ h(ID_{G'}, |G'|, ID_G, |G|) & ID_G > ID_{G'} \end{cases} \tag{2}$$

4.4 GVT Formation

There will be one GVT per group. The GVT leaves are IDs of nodes in the group. Internal nodes represent intermediate group IDs. Each node maintains information about its branch of the GVT specifically, the group ID and size of each merge partner.

4.5 GVT Verification

Before merging, group G verifies the GVT for G' (and vice versa). G' announces its group ID (and size). Group G sends a challenge value to G'. The challenge uniquely selects a node in G'. Chosen node sends its certificate and GVT information to G. Nodes in G verify the GVT values [11]. By this mechanism all are verified to be non malicious nodes. During the convergence of the GVT mechanism the verification process automatically eliminates malicious nodes in the sensor network and the authentication is denied for malicious nodes.

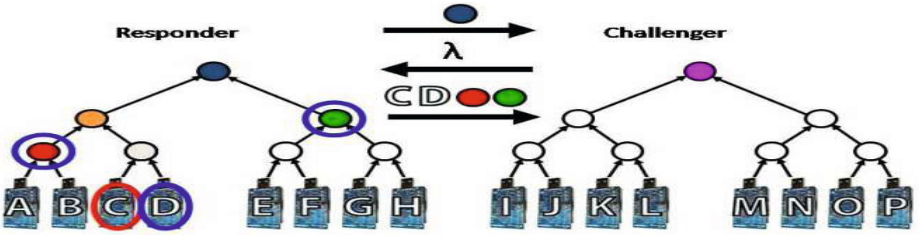

Fig. 2. Response and Challenge Scenario of Sensor Nodes

4.6 Eliminating Malicious Nodes

To legitimate nodes we used the Honeybee mechanism to eliminate malicious nodes. To revoke malicious node M, legitimate node L broadcasts: IDL, IDM, and a signature legitimate nodes revoke M *and* L. It prevents a compromised node from revoking more than one legitimate node.

5 Simulations

We made comparison against Beacon Vector Routing (BVR) protocol [NSDI 2005] with energy saving in mind [8]. It is optimized for efficiency. Experimental Setup for 500 nodes, random deployment, DOI radio model are made to achieve our results. Summary of our Results are:

- Paths longer than shortest path
- Distributes overhead evenly throughout network
  - Better than BVR, even in topologies with voids
- Our routing success rate is 100% as it is a trade between speed and security. It is because of low weight cryptography (Stream Ciphers) and use of Hash Function which has time complexity of O(1).

5.1 Metric: Path Stretch

Stretch = Protocol Path Length / Optimal Path Length.
Optimistic for BVR: does not include failed BVR routes.

5.2 Implementation

We developed in NesC on TinyOS using Telos sensor nodes with source code to be available soon. The challenges overcome with (i) Reliable Broadcast (ii) A synchronicity (iii) Asymmetric Links. Ongoing work to expand the current test bed.

5.3 Validation

Our proposed research work is different and unique from the previous work done on sensor routing. As the verification during the convergence in the GVT mechanism authentication is denied for malicious nodes. Second because of low weight cryptography (stream ciphers) less computational time is required due to which less energy is required for sensor routing networks. More over our solution is more valid due to usage of Hash Function which has computational complexity of O(1), which is fastest for measuring the speed of convergence.

6 Critiques and Future Work

Following critiques and suggestions came after thorough analysis of relevant papers.

1. This paper used Tree for verification of nodes and emerged with algorithm i.e. **GVT** (Group Verification Tree), so that illegitimate sensor devices could not enter into the network as an intruder. This algorithm can be made more enhanced and efficient by using Hash function rather than trees. This will exponentially increase its routing information convergence process with less minimum runtime if memory is provided to maintain hash table.
2. As for as security is concerned, sensor device may be incorporated and embedded with a chip with secure encrypted ID .This encryption can be done using any Asymmetric or Symmetric cryptography(Public Key Cryptography). I proposed stream cipher to be more suitable for this system because of light weight cryptography and good avalanche effect of sensors and wireless networks.
3. The secure routing protocol should be introduced to combat the hidden terminal problem.
4. The protocol should use (less control messages).e.g. RREQ. (Route Request)
5. The computational power of the algorithm should be less to save the sensor *Node Energy* [4]
6. If the above suggestions are brought into consideration, then IEEE Standard 802.11.15.4 can be further improved and enhanced.

7 Conclusions

To secure sensor routing is an important and difficult problem. Most previous techniques assume a trusted environment or use a single security technique. The authors designed a protocol incorporating all three security techniques that still compares favorably to insecure protocols.

Acknowledgment

We are thankful to Chairman of Department of Information Systems, Dean of College of Computer and Information Sciences, Center of Excellence in Information Assurance, King Saud University for their cooperation and support.

References

1. Xiao, D., Wei, M., Zhou, Y.: Secure-SPIN: Secure Sensor Protocol for Information via Negotiation for Wireless Sensor Networks. In: 1ST IEEE Conference on Industrial Electronics and Applications, pp. 1–4 (2006), doi:10.1109/ICIEA.2006.257149
2. IEEE 64th Vehicular Technology Conference VTC 2006, pp. 1–5 (Fall 2006), doi:10.1109/VTCF.2006.505
3. Akyildiz, S., et al.: Wireless Sensor Networks: A Survey (2002)
4. Ganesan, D., et al.: Highly Resilient, Energy-Efficient Multipath Routing in Wireless Sensor Networks. Mobile Comp. and Commun. Review 5(4), 10–24 (2002)
5. Hu, Y.-C., Perrig, A., Johnson, D.B.: Packet Leashes: A Defense Against Wormhole Attacks in Wireless Networks. In: Proc. IEEE INFOCOM (2003)

6. Parno, B., Luk, M., Gaustad, E., Perrig, A.: Secure Sensor Network Routing: A Clean Slate Approach (2006)
7. Chan, H., Perrig, A., Song, D.: Random Key Predistribution Schemes for Sensor Networks. In: Proceedings of the 2003 IEEE Symposium on Security and Privacy, May 11-14, p. 197 (2003)
8. Tejaswi, K., Mehta, P., Bansal, R., Parekh, C., Merchant, S.N., Desai, U.B.: Routing Protocols for Landslide Prediction using Wireless Sensor Networks (2006)
9. Roy, S., Setia, S., Jajodia, S.: Attack-resilient hierarchical data aggregation in sensor networks. In: Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks, Alexandria, Virginia, USA, October 30 (2006)
10. Chan, H., Perrig, A., Przydatek, B., Song, D.: SIA: Secure information aggregation in sensor networks. Journal of Computer Security 15(1), 69–102 (2007)
11. Srinivasan, A., Wu, J.: A novel k-parent flooding tree for secure and reliable broadcasting in sensor networks. In: Proceedings of IEEE International Conference on Communications—Computer and Communications Network Security, ICC CCN (2007)
12. Srinivasan, A., Wu, J.: Secure and reliable broadcasting in wireless sensor networks using multi-parent trees. In: Security Comm. Networks, Wiley InterScience, Hoboken (2008)
13. Roman, R., Lope, J.: Integrating wireless sensor networks and the internet: a security analysis. Journal of Internet Research 19(2), 246–259 (2009)