ISSN:0975-9646

Dynamic Routing Key Distribution in Security Considerations

Dr. D. Raghu, MD. Baliguddin, Ch. Raja Jacub
CSE Dept., Nova College of Engineering & Technology,
Jangareddigudem, Andhra Pradesh, INDIA

ABSTRACT – In wireless network to protect the sensitive data Security has become one of the major issues for data communication over wired and wireless networks. Different from the past work on the designs of cryptography algorithms and system infrastructures, we will propose Key Distribution scheme for hierarchical WANs with renewable network devices. Applying the key distribution in the dynamic routing algorithm it will be provide the more scalability and security in the wireless networks.

KEYWORDS – RIP, WSN$_S$, KDS, S.P.F.

INTRODUCTION

The security in wireless sensor networks. Current proposals for routing protocols in sensor networks optimize for the limited capabilities of the nodes and the application specific nature of the networks, but do not consider security. Although these protocols have not been designed with security as a goal, we feel it is important to analyze their security properties. When the defender has the liabilities of insecure wireless communication, limited node capabilities, and possible insider threats, and the adversaries can use powerful laptops with high energy and long range communication to attack the network, designing a secure routing protocol is non-trivial. The alternative for security-enhanced data transmission is to dynamically route packets between each source and its destination so that the chance for system break-in, due to successful interception of consecutive packets for a session, is slim. The intention of security-enhanced routing is different from the adopting of multiple paths between a source and a destination to increase the throughput of data transmission (see, e.g., [8] and [9]). In particular, Lou et al. proposed a secure routing protocol to improve the security of end-to-end data transmission based on multiple path deliveries. The set of multiple paths between each source and its destination is determined in an online fashion, and extra control message exchanging is needed. Bo hacek et al. [2] proposed a secure stochastic routing mechanism to improve routing security. Similar to the work proposed by Lou et al. [14], [15], a set of paths is discovered for each source and its destination in an online fashion based on message flooding. Thus, a mass of control messages is needed. the trading of the security level and the traffic dispersion. They proposed a traffic dispersion scheme to reduce the probability of eavesdropped information along the used paths provided that the set of data delivery paths is discovered in advance. Although excellent research results have been proposed for security-enhanced dynamic routing, many of them rely on the discovery of multiple paths either in an online or offline fashion. For those online path-searching approaches, the discovery of multiple paths involves a significant number of control signals over the Internet. On the other hand, the discovery of paths in an offline fashion might not be suitable to networks with a dynamic changing configuration. Therefore, we will propose a dynamic routing algorithm to provide security-enhanced data delivery without introducing any extra control messages.

BACKGROUND

We present some background on structured p2p overlay protocols like CAN, Chord, Tapestry and Pastry. Space limitations prevent us from giving a detailed overview of each protocol. Instead, we describe an abstract model of structured p2p overlay networks that we use to keep the discussion independent of any particular protocol. For concreteness, we also give an overview of Pastry and point out relevant differences between it and the other protocols. Next, we describe models and assumptions used later in the paper about how nodes might misbehave. Finally, we define secure routing and outline our solution. Throughout this paper, most of the analyses and techniques are presented in terms of this model and should apply to other structured overlays except when otherwise noted. However, the security and performance of our techniques was fully evaluated only in the context of Pastry; a full evaluation of the techniques in other protocols is future work

KEY DISTRIBUTION

We present the foundations and basic idea of our key distribution scheme based on a three-tier hierarchal network model. *Key Distribution in Renewable WSNs.* Specifics of wireless sensor networks, such as strict resource constraints and large network scalability, require a proposed security protocol to be not only secure but also efficient. Recent research shows that preloading symmetric keys into sensors before they are deployed is a practical method to deal with the key distribution and management problem in wireless sensor networking environments. After the deployment, if two neighboring nodes have some common keys, they can setup a secure link by the shared keys. As surveyed in [9], the existing schemes can be classified into the following three categories: random key pre-distribution schemes,

polynomial-key pre-distribution schemes, and location-based key pre-distribution schemes. In our key distribution scheme, a key distribution server (KDS) is available for both of the following cases. (1) KDS is installed in the base station, by which the keys can be delivered instantaneously when the BS is on-line to the requester. (2) It is available to the network deployer when the keys are required to be preloaded into network devices. In many applications, new network devices need to be replenished into an already deployed network to replace the power-exhausted or compromised devices. The corresponding key management should be provided in order to setup the secure link between a new added network device and an existing one. To our best knowledge, there are no full solutions to the dynamic membership management for key distribution in hierarchal WSNs with renewable cluster head and sensor node. For example, some of them can only support the sensor node addition in the case when BS is online. The objective of our key distribution protocols is to provide a complete and flexible solution for such renewable WSNs. In particular, we will provide the key distribution protocols for both sensor node and cluster head when the BS is on-line or off-line. *Symmetric Polynomial Function.* In our key distribution scheme, a bivariate Symmetric Polynomial Function (s.p.f.) is used to generate the key for each link of the network. The *t*-degree bivariate symmetric polynomial function $f(x, y)$, introduced in [12], is defined as $f(x,y) = t; i, j=0; a_{ij}, x_i, y_j$. (1) The coefficients a_{ij} $(0 \le i, j \le t)$ are randomly chosen from a finite field $GF(Q)$, in which Q is a prime number that is large enough to accommodate a cryptographic key. As implied by its name, the symmetric property of a bivariate polynomial function satisfies $f(x, y) = f(y, x)$. In our key distribution scheme, the KDS maintains two bivariate polynomial functions: (i) the s.p.f. fCH-NS(x, y) is used to establish the key between existing cluster head and new sensor node, (ii) the s.p.f. fCH-NCH(x, y) is used to establish the key between existing cluster head and new cluster head.

DYNAMIC ROUTING WITH KEY DISTRIBUTION

Key Distribution algorithm for dynamic routing to improve the security of data transmission. We propose to rely on existing distance information exchanged among neighboring nodes (referred to as routers as well in this paper) for the seeking of routing paths. In many Key Distribution -based implementations, e.g., those based on RIP, each node N_i maintains a routing table (see Table 1a) in which each entry is associated with a tuple t, $W_{N_i,t}$, Nexthop; where t, $W_{N_i,t}$ and Nexthop denote some unique destination node, an estimated minimal cost to send a packet to t, and the next node along the minimal-cost path to the destination node, respectively. With the objective of this work in the randomization of routing paths, the routing table shown in Table-1a is extended to accommodate our security-enhanced dynamic routing algorithm. In the extended routing table, we propose to associate each entry with a tuple t; $W_{N_i,t}$; $C_{N_i,t}$; $H_{N_i,t}$. $C_{N_i,t}$ is a set of node candidates for the nexthop (note that the candidate selection will be elaborated, where one of the nexthop candidates that have the minimal cost is marked. $H_{N_i,t}$, a set of tuples, records the history for packet deliveries through the node N_i to the destination node t. Each tuple Nj; H_{N_j} in $H_{N_i,t}$ is used to represent that N_i previously used the node H_{N_j} as the nexthop to forward the packet from the source node N_j to the destination node t. Let $N_{b_r,i}$ and W_{N_i,N_j} denote the set of neighboring nodes for a node N_i and the cost in the delivery of a packet between Ni and a neighboring node N_j, respectively. Each node N_i also maintains an array (referred to as a link table) in which each entry corresponds to a neighboring node Nj 2 $N_{b_r,i}$ and contains the cost W_{N_i,N_j} for a packet delivery.

RANDOMIZATION

Consider the delivery of a packet with the destination t at a node Ni. In order to minimize the probability that packets are eavesdropped over a specific link, a randomization process for packet deliveries shown in Procedure 1 is adopted. In this process, the previous nexthop hs (defined in $H_{N_i,t}$ t) for the source node s is identified in the first step of the process. Then, the process randomly picks up a neighboring node in $C_{N_i,t}$ excluding hs as the nexthop for the current packet transmission. The exclusion of hs for the nexthop selection avoids transmitting two consecutive packets in the same link, and the randomized pickup prevents attackers from easily predicting routing paths for the coming transmitted packets.

1 RANDOMIZEDSELECTOR (S; T; PKT)

1: Let h_s be the used nexthop for the previous packet delivery for the source node s.

2: **if** $h_s \varepsilon\ C_t^{N_i}$ then

3: **if** $\left| C_t^{N_i} \right| > 1$ then

4: Randomly choose a node x from $\left\{ C_t^{N_i} - h_s \right\}$ as a nexthop, and send the packet pkt to the node x.

5: $h_s \leftarrow$ x, and update the routing table of N_i

6: **else**

7: Send the packet pkt to h_s

8: **end if**

9: **else**

10: Randomly choose a node y from $C_t^{N_i}$ as a nexthop, and send the packet pkt to the node y.

11: $h_s \leftarrow$ y, and update the routing table of N_i.

12: **end if**

PERFORMANCE EVALUATION

Now we turn our attention to evaluate the performance of this group of key distribution schemes in hierarchical WSNs. The performance metrics are storage and communication overhead. To supports a large-scale WSN, a feasible solution of key distribution should be scalable in terms of storage cost. In the scheme LEKM [10], the number of keys stored in each CH is linearly proportional to the number of clusters. The IKDM scheme has fixed storage overhead for sensor nodes and cluster heads. Our scheme has fixed storage cost for sensor nodes. The storage requirement O (λS + λCH) for cluster head is also reasonable because it requires to communicate with at least λS+λCH number of nodes. The performance comparison in various network sizes is summarized. the cluster head addition processes, the communication overhead of Protocols 2 and 4 is both fixed under the condition that λS and λCH are constant numbers, which is true for a uniform node deployment. This feature shows the scalability of our scheme in terms of message complexity. They are also the first solution for key management in WSNs with renewable cluster heads. In the following, we conduct a simulation study on the communication overhead for the sensor node addition process. We have implemented a simulation tool using Java for the special purpose of evaluating the performance of this group of protocols while the lower MAC layer is assumed to be ideal. A hierarchical wireless sensor network was simulated with different sizes of n sensor nodes and m clusters. In order to study the scalability of these protocols, we have considered the scenarios with a specified a cluster size m (m = 9, 16, 25, 36, 49, 64, 81, and 100) and a sensor node size n (n = 100 m). For each example, the whole network is regularly organized as $\sqrt{m} \times \sqrt{m}$ number of clusters, and there are exactly 100 sensor nodes in each $R \times R$ cluster. The transmission range of each cluster head is set as $\sqrt{5}R$, and the communications between CHs may be made in a multihop manner if they are separated far away from each other. To simulate the sensor node addition process, we consider 10 new sensor nodes to be added to each cluster. In each message interaction for all protocols, the length of each Id and key takes up 32 and 80 bits, respectively. The performance comparison is made in terms of communication overhead. It is evaluated in the number of bits transmitted for key establishment between a sensor node and a cluster head. In all cases, that is, a sensor node size n, a cluster size m, and a specific key distribution scheme, we randomly generated 50 different instances and we present here the average over those 50 instances. scheme has the fixed and lowest communication overhead for the on-line scenario. The experimental results also comply with our protocol design for the off-line scenario, in which multiple candidate proxies can improve the performance, that is, the communication overhead is a decreasing function of under fixed network size. In summary, our scheme in both scenarios can significantly outperform other proposals.

CONCLUSION

The security-enhanced dynamic routing algorithm based on distributed routing information widely supported in existing networks. The proposed algorithm is easy to implement and compatible with popular routing protocols with flexible key distribution scheme based on three-tier renewable wireless sensor networks. Our scheme can defend against node capture attack and support dynamic membership management. To our best knowledge, the solution of the key establishment for new cluster heads under both the BS off-line and online cases is proposed by the first time. Furthermore, our scheme is efficient and scalable in terms of communication and storage costs, which is particularly beneficial to support large-scale and resource constrained WSNs.

REFERENCES

[1] G. Apostolopoulos, V. Peris, P. Pradhan, and D. Saha, “Securing Electronic Commerce: Reducing the SSL Overhead,” IEEE Network, 2000.

[2] S. Bohacek, J.P. Hespanha, K. Obraczka, J. Lee, and C. Lim, “Enhancing Security via Stochastic Routing,” Proc. 11th Int’l Conf. Computer Comm. and Networks (ICCCN), 2002.

[3] D. Collins, Carrier Grade Voice over IP. McGraw-Hill, 2003.

[4] T.H. Cormen, C.E. Leiserson, and R.L. Rivest, Introduction to Algorithms. MIT Press, 1990.

[5] P. Erdo¨s and A. Re´nyi, “On Random Graphs,” Publicationes Math. Debrecen, vol. 6, 1959.

[6] M. Faloutsos, P. Faloutsos, and C. Faloutsos, “On Power-Law Relationships of the Internet Topology,” Proc. ACM SIGCOMM’99, pp. 251-262, 1999.

[7] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: a survey,” Computer Networks, vol. 38, no. 4, pp. 393–422, 2002.

[8] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” Communications of the ACM, vol. 21, no. 2, pp. 120–126, 1978.

[9] W. Diffie and M. E. Hellman, “New directions in cryptography,” IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644–654, 1976.

[10] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, “An application-specific protocol architecture for wireless microsensor networks,” IEEE Transactions on Wireless Communications, vol. 1, no. 4, pp. 660–670, 2002.

[11] L. Eschenauer and V. D. Gligor, “A key-management scheme for distributed sensor networks,” in Proceedings of the ACM Conference on Computer and Communications Security (CCS ’02), pp.41– 47, Washington, DC, USA, November 2002.