IJCSN - International Journal of Computer Science and Network, Volume 6, Issue 4, August 2017
ISSN (Online): 2277-5420
www.IJCSN.org
Impact Factor: 1.5

Security Services in Group Communications over Mobile Ad-Hoc and Wireless Sensor Networks Using Performance Analysis of Algorithms

Ramkumar Ramaswamy

Department of Computer science and Information Technology, DMI-St. John the Baptist University,
Mangochi, The Republic of Malawi

Abstract - Group communications in wireless networks has been facilitating many emerging applications that require packet delivery from one or more sender(s) to multiple receivers.. Due to insecure wireless channels, group communications are susceptible to various kinds of attacks. Although a number of proposals have been reported to secure group communications using Group management key (GMK), provisioning security in group communications in wireless networks remains a critical and challenging issue. This article presents a survey of recent advances in security requirements and services in group communications in three types of wireless networks, and discusses challenges in designing secure group communications in these networks: wireless infrastructure networks, mobile ad hoc networks, and wireless sensor networks. This article presents a survey of recent advances in security requirements and services in group communications in three types of wireless networks, and discusses challenges in designing secure group communications in these networks: wireless infrastructure networks, mobile ad hoc networks, and wireless sensor networks.

Keywords - *WSN, Security Service*

1. Introduction

Many Wireless Sensor Networks (WSNs) are being en-visage in military, emergency and surveillance applications today, where sensor nodes need to send sensed data to the sink. In many applications under hostile environment, sensor nodes cannot be deployed deterministically and thus are randomly deployed into the field. An important requirement in network management of many mission critical applications is to secure end to end sensor networks data from being eavesdropped by the attacker. While there have been many works devoted to hop by hop secure communications in WSNs, the issue of end to end secure communications is largely ignored. This is mainly due to the fact that there exist two intuitive approaches to provide a high degree of end to end secure communications. Mobile ad hoc networks are formed by a collection of, potentially mobile, wireless nodes; communication links form and disappear as nodes come into and go out of each other's communication range. Wireless networking has received a boost from the development of standards such as IEEE 802.11 and Bluetooth. Much of this activity has focused on the design of routing and medium access control protocols, since efficiency of these protocols can have a significant impact on performance.

2. Group Communication

A group communication service forms an important building block for applications in dynamic distributed systems and is useful in many applications that involve collaborations among a group of people. The key features of a group communication service are:

(1) Maintaining information regarding group membership.
(2) Letting nodes within a group communicate with each other in an ordered manner.
There has been significant research activity on group communication in traditional wired networks. The vast body of this research is an indicator of the significance of the group communication service paradigm.

2.1 Approaches Used For Total Ordered Node Delivery

Group communication services have been successfully used in the past as building blocks and abstractions for

implementing distributed tasks. Past work on total ordering has yielded several approaches which use a token to implement the total order. These algorithms have two flavors: As exemplified by the algorithms, totally ordered message delivery is achieved by continually circulating a token through all the nodes of the network in a virtual ring.

2.2 Tokens Carrying Sequence Numbers

The token circulates around the virtual ring carrying a sequence number. When a node receives the token, it assigns sequence numbers (carried with the token) to its messages, and then multicasts the messages to the group members. The sequence number carried in the token is incremented once for each message sent by the node holding the token. Since the messages are assigned globally unique sequence numbers, total order can be achieved.

2.3 Tokens Carrying Messages

An alternative approach is to store the messages in the token itself – since the token visits all nodes in a virtual ring, the messages will eventually reach all the nodes, the order in which messages are added to the token determining the order in which they are delivered to the nodes. Both these approaches depend on the existence of a virtual ring in the network. But the prior work has not sufficiently addressed the issue of determining efficient embeddings of rings in networks with dynamically changing topology.

2.4 Static Vs Dynamic

The topology is said to be static, when there is no mobility. Whereas when there is mobility, the topology is said to be dynamic. There are several mechanisms for finding approximations to a virtual ring that change dynamically as the topology changes and that are efficient according to certain metrics. Since token circulation around a virtual ring is a useful component of many existing group communication mechanisms for wired networks, we will consider ways of improving the performance of such mechanisms in mobile ad hoc networks.

3. Group Key Management (GKM)

The fundamental security service in SGC is the provision of a shared key, the group key. The shared group key is used to encrypt a group message, sign the message, authenticate members and messages, and authorize access to traffic and group resources. Thus, the strength of SGC largely relies on the cryptographic strength of the keys and the key management protocol. A GKM scheme deployed in any secure group communication system should satisfy the following requirements:

# of shared keys	0	1	2	3	4
# of links increase	54%	–8%	–20%	–29%	–19%
# of shared keys	5	6	7	8	>8
# of links increase	–2%	25%	56%	183%	475%

TABLE-I

Increase of the Number of Links with Different Number of Shared Keys under Differentiated Key Pre-Distribution

- Key generation is secure.
- Imitation of the group key should be infeasible or computationally difficult.
- The group key is securely distributed and only the legitimate users can receive a valid group key.
- Revocation of the group key upon every membership change should be immediate.
- Every membership change must result in rekeying of associated keys.
- A rekeying of the key is secure.

3.1 Group authentication

In group communication (one-to-many and many-to-many), a member can be the designated sender, the designated receiver, or both. Both users and messages should be authenticated to safeguard identity related attacks. In some systems a member certificate is issued by the trusted certificate issuing entity along with its validation period. In some systems the expired certificate is maintained for further verifications. Expired certificates are compiled into the revocation list, which is distributed to notify all members. Group authorization and access control: In any conventional access control mechanism, a member who holds a decrypting key can access full contents in a flow (or all flows in an aggregated stream). This is referred to as a single access privilege.

3.2 Group accounting and no repudiation

Any group operation executed or a record of resources utilized by a member should be available for tracking in

order to detect any abusive usage of resources and operations. A no repudiation service can ensure that the identity of a member whose activities are in dispute can be fully and precisely determined by the designated entity. In general, the group signature and member certificate can be used to authenticate the source and message, and to provide proof of the source's activity in case of a dispute.

3.3 Group privacy and anonymity

Any information related to a group message, such as identities of a sender and a receiver, message length, and time, can be protected or hidden to preserve privacy and anonymity of members. An anonymous message refers to a message that carries no information about the senders and receivers.

3.4 Group message integrity and confidentiality

Message integrity should be preserved by ensuring that the message has not been fabricated (some or all portions of the message have not been added, deleted, or modified) or dropped by an unauthorized entity. This can be done by several means, including hashing and signing the message along with strong encryption keys. In ad-hoc networks, group members may have different capabilities and protocols to perform different levels of encryption on group messages. Thus, some messages may be encrypted with strong encryption, while others with weak encryption are relatively easily breakable. In WSNs sensor nodes may have similar capabilities and protocols that are embedded before deployment. Confidentiality ensures that only authorized members can retrieve meaningful data from the message.

3.5 Group survivability and availability

An attacker can attack routing hosts (i.e., access points and base stations) to isolate some or all group members, or partition the group. Thus, all routing hosts must be protected to ensure group survivability. However, the attacker can still target a joining procedure (i.e., by flooding the access point or base station in wireless infrastructure networks and WSNs), thus causing service unavailability to other legitimate users. Group availability ensures that only authorized users can always communicate within the group by using restricted group resources, and any violation exceeding the limitation of group resources will be promptly detected. Thus, flooding packets would be dropped immediately once such an attack has been detected. Unauthorized routing update can be detected and prevented by the following services: authenticating both source and message to determine whether the routing update message is legitimate and originated by an authorized member; enforcing access control over a routing table; signing the routing update message such that message integrity is preserved and no attacker has falsely modified the message; encrypting all management packets (routing update requests and replies); and any loophole or sinkhole routing, which possibly leads to a denial of service, will be tested, detected, and fixed prior to actual deployment.

4. Routing Protocols in WSNs

Routing in wireless sensor networks has some differences from that in traditional wired and wireless ad-hoc networks due to resource constraints, faults/failures etc. There are two main paradigms of routing protocols in WSNs: location-centric routing and data-centric routing. Other paradigms include hierarchical routing and security aware routing.

4.1Location-centric routing

Greedy Perimeter Stateless Routing (GPSR) is a well known location centric routing protocol. In GPSR, beacon messages are broadcast by each node to inform its neighbors of its position. GPSR assumes that sensors can determine through separate means the location of the sink. Each node makes forwarding decisions based on the relative position of the sink and its neighbors. In general, the neighbor that is closest to the sink is chosen.

4.2 Data-centric routing

Directed diffusion is the most well known data centric routing protocol, in which the sink sends queries to all nodes and waits for data from the nodes Satisfying specific requirement. In order to create a query, an interest is defined using a list of attribute-value pairs such as name of objects, geographical area, etc.

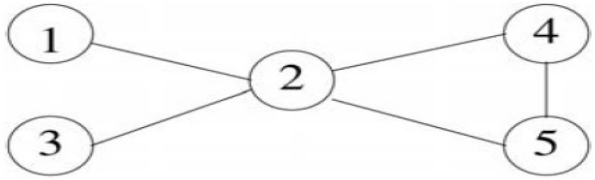

Fig: 1. Data Centric Routing

The interest is broadcast through the network, and used by each node to compare with the data received. The interest entry also contains several gradient fields. A gradient is a reply link to a neighbor from which the interest was received. By utilizing interests and gradients, paths are established between sensors and the sink. Several paths may be established, and one of them is selected by reinforcement.

5. User Interface

Initially setup the network simulator model using java swing concepts. It will be displayed the number of nodes and regions in different colors for user reference. GUI also displays the performance measurements, time, and speed and display graph also.

6. Local-Frequency (LF)

The Local-Frequency (LF) algorithm keeps track of how many times each node has been visited and sends the token to the least frequently visited neighbor of the token-holder. To implement this algorithm, the count, for each node, as stored in the token, contains the number of past token visits to that node. The token-holder may not have a precise knowledge of its neighbors; occasionally the chosen node may no longer be its neighbor. To protect against the potential loss of the token in such cases, we use a TCP connection to deliver the token. There is no mobility and the topology is connected, then the LF algorithm ensures that every node is visited infinitely. i.e., there is no starvation. The LF algorithm has the unfortunate property that the round length can increase without bound in certain network topologies, even if there is no mobility.

7. Local-Frequency (LF)

The Local-Frequency (LF) algorithm keeps track of how many times each node has been visited and sends the token to the least frequently visited neighbor of the token-holder. To implement this algorithm, the count, for each node, as stored in the token, contains the number of past token visits to that node. The token-holder may not have a precise knowledge of its neighbors; occasionally the chosen node may no longer be its neighbor. To protect against the potential loss of the token in such cases, we use a TCP connection to deliver the token. There is no mobility and the topology is connected, then the LF algorithm ensures that every node is visited infinitely. i.e., there is no starvation. The LF algorithm has the unfortunate property that the round length can increase without bound in certain network topologies, even if there is no mobility. Initially, the token resides at node 1. Assume that the LF algorithm breaks ties in favor of the neighboring node with the smallest identifier. In this case, it is easy to verify that the length of a round will grow unboundedly with time, when using the LF algorithm.

8. Performance Evaluation

In this section, we present performance evaluation based on both analysis and simulation. We first describe our simulation setup, and then report performance data and our observations.

8.1 Simulation Setup

The network is circular with radius 500 meters, where 1000 nodes are uniformly deployed at random. The sink is at the center of the network. Unless otherwise specified, the default parameters are: $c = 2$, $n1 = 200$, $n2 = 800$, $k1 = 80$, $k2 = 30$, $k = 40$, $K = 10000$, $r = 100$ meters, $\alpha = 1$ and $Nc = 50$ The default values of $k1$, $k2$ and k are chosen such that $k1n1/(n1+n2)+k2n2/(n1+n2) = k$, which means the average number of keys disclosed to the attacker is the same in our differentiated key pre-distribution and the original *RKP* scheme for the same number of captured nodes. Our communication model is one where sensors periodically transmit data to the sink. In the legend in all figures, our GPSR and our minhop refer to our protocols extending GPSR [45] and minimum hop [50] routing present. The legends GPSR and Minhop refer to the traditional GPSR and minimum hop routing protocols following the uniform key pre-distribution respectively. Each point in the simulation data is the average of 100 runs based on independent random seeds.

8.2 Sensitivity of Pe2e to Attack Intensity

First compare our differentiated key pre-distribution with the traditional uniform key pre-distribution (for both GPSR and minimum hop routing protocols) under different number of captured nodes *Nc*. We find that while the performance of all schemes degrades with increasing *Nc*, our schemes are consistently better than those of traditional schemes. We also find that the improvement increases with larger values of *Nc*. This is because when the attacker captures more nodes, the resilience of highly resilient links in our schemes

degrades at a much slower pace than those of the less resilient links in traditional schemes. Besides, we can also observe that the end to end security under minimum hop based protocols is better than their GPSR counterparts.

8.3 Sensitivity of Pe2e to Network Density

We can compare our schemes and traditional schemes under different communication range *r*, which in turn corresponds to different network density (i.e., number of neighbors per node).

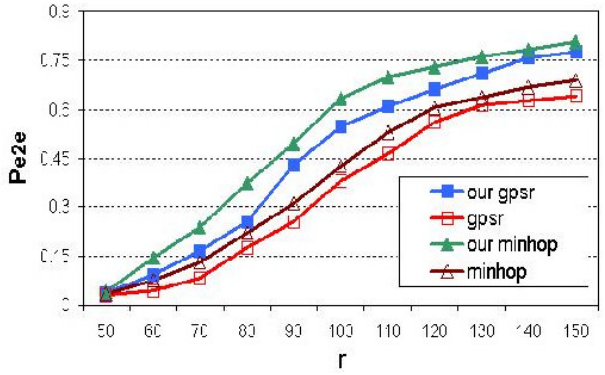

Fig: 2. Sensitivity of P_{e2e} to communication range *r*.

When *r* is small, *Pe2e* is low due to both low connectivity (many nodes cannot find secure neighbors) and low resilience (fewer proxies resulting in fewer key paths for each link). When *r* increases, *Pe2e* increases correspondingly. For all values of *r*, our schemes perform consistently better.

8.4 Sensitivity of network lifetime to parameter

Recall that α is the *knob* that trades-off security with lifetime. We compare our schemes and the traditional schemes for different values of α. We define network lifetime as the time until when the first node has used up its energy. Since traditional schemes do not have weight assignment, they are insensitive to α. The lifetime in our schemes decreases with larger values of α. This is because a larger value of α means more priority is given to links with high resilience, thereby draining the corresponding neighbors more rapidly. We also observe that the extended GPSR has higher lifetime compared with extended minimum hop for smaller values of α, and the difference diminishes as α increases. This is because for smaller values of α, lifetime is mainly decided by total number of candidate forwarders of each node. In extended GPSR, each node usually can find more forwarders (secure neighbors closer to sink) than it can find in extended minimum hop protocol (secure neighbors on minimum hop secure path).

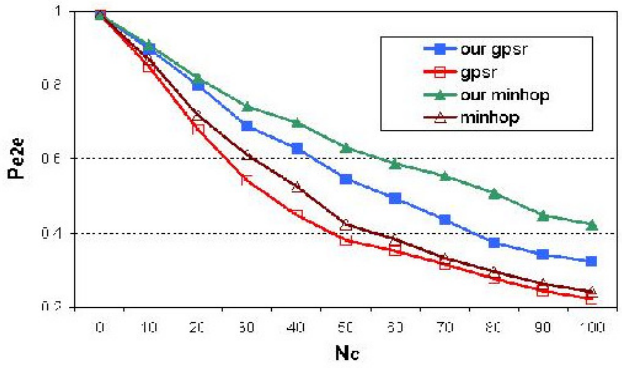

Fig: 3. Sensitivity of P_{e2e} to number of captured nodes N_c.

When α increases, lifetime is mainly decided by the number of most secure neighbors of each node. This number is similar for both protocols, and hence they have similar lifetimes when α increases. We also observe that lifetime of traditional GPSR scheme is lower than that of traditional minimum hop scheme.

Sensitivity of Pe2e and network lifetime to number of class 1 nodes*:*

We compare the traditional schemes, our schemes with default parameters, and our schemes with optimal parameters. The optimal parameters are obtained via our analysis.

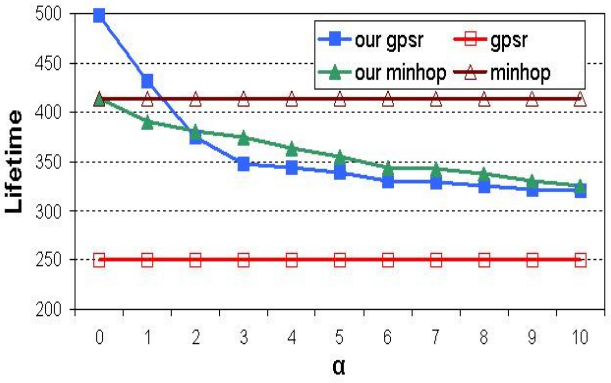

Fig: 4. Sensitivity of lifetime to parameter

The average number of keys pre-distributed per node is the same across all schemes for fairness of comparison. we find that traditional schemes are insensitive to n_1 since all nodes are given same number of keys. Our schemes

achieve much better performance under intermediate values of n_1, while the performance of our schemes is close to that of traditional schemes for very small and very large values of n_1. This is because when n_1 approaches 0 or 1000, all nodes will be given same number of keys, and thus our schemes degrade to traditional schemes.

9. Conclusion

Nowadays, most of the network system is established in the mobile environments. Every mobile ad hoc system should be accessed with the better performance. In this proposed system "Distributed Token Ring circulation in mobile Ad-hoc Networks", to measure the performance of the local and global connectivity between the nodes. An important application of such algorithms is to ensure total order of message delivery in a group communication service. If the algorithms are gives different performance results for each group in the ad hoc network topology. When using a token circulation algorithm, a round is said to complete when every node has been visited at least once. Criteria for comparing the algorithms include the average time required to complete a round, number of bytes sent per round, and number of nodes visited per round.

References

[1] S. K. S. Gupta and S. Cherukuri, "An Adaptive Protocol for Efficient and Secure Multicasting in IEEE 802.11 Based Wireless LANs," Proc. IEEE WCNC 2003, vol. 3, Mar. 2003, pp. 2021–26.

[2] A. Wadaa et al., "On Providing Anonymity in Wireless Sensor Networks," Proc. 10th Int'l. Conf. Parallel and Distrib. Syst., July 2004, pp. 411–18.

[3] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Elsevier's Ad Hoc Networks J., Special ssueI on Sensor Network Applications Protocols, vol. 1, no. 2–3, Sep. 2002, pp. 293–315.

[4] R. Maheshwari, J. Gao, and S. R. Das, "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information," Proc. IEEE INFOCOM '07, Mar.2007.

[5] B. Decleene et al., "Secure Group Communications for Wireless Networks," Proc. IEEE MILCOM 2001, vol. 1, Oct. 2001, pp. 113–17.

[6] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," Proc. 10th ACM Conf. Computer and Communication Security, Oct. 2003, pp. 62-72.

[7] Z. Yu and Y. Guan, "A Robust Group-Based Key Management Scheme for Wireless Sensor Networks," Proc. IEEE WCNC '05, vol. 4, Mar. 2005, pp. 1915–20.

[8] W. Zhang and G. Cao, "Group Rekeying for Filtering False Data in Sensor Networks: a Predistribution and Local Collaboration-Based Approach," *Proc. IEEE INFOCOM '05*, vol. 1, Mar. 2005, pp. 503–14.

[9] M. Striki and J. Baras, "Towards Integrating Key Distribution with Entity Authentication for Efficient, Scalable and Secure Group Communication in MANETs," *Proc.IEEE ICC '04,* vol. 7, June 2004, pp. 4377–81.

[10] R. K. Balachandran *et al.*, "CRTDH: An Efficient Key Agreement Scheme for Secure Group Communications in Wireless Ad Hoc Networks," *Proc. IEEE ICC '05*, vol. 2, May 2005, pp. 1123–27.