International Journal of Computer Science and Network (IJCSN)
Volume 1, Issue 4, August 2012 www.ijcsn.org ISSN 2277-5420

Secured Routing Protocols for Wireless & ATM Networks : An Analysis

[1]Sanyam Agarwal ,[2] Dr.A.K.Gautam

[1]Research Scholar ,Deptt. Of Electronics , India

[2]S.D.College Of Engineering. & Technology, Deptt. Of Electronics ,MuzaffarNagar, (U.P.)-251001

Abstract

Routing protocols in WSNs might differ depending on the application and network architecture. Routing protocols that do not take the malicious attacks into account cannot be easily tamper proofed. Wireless sensor networks consist of small nodes with sensing, computation, and wireless communication capabilities. Many routing, power management, and data dissemination protocols have been specifically designed for WSNs where energy awareness is an essential design issues. These protocols should be designed securely so that they are capable of asserting countermeasures whenever they need to. This paper is an effort to evaluate the most important security factors in wireless sensor networks. Then, based on these factors and the application type of the routing protocols, we compare the vulnerability of different groups of protocols.

Keywords *— Security Factors, Wireless sensor networks*

1. INTRODUCTION

In multi-hop wireless systems, such as ad-hoc and sensor networks, the need for cooperation among nodes to relay each other's packets exposes them to a wide range of security attacks. Also, routing is a fundamental functionality in wireless sensor networks, thus hostile interventions aiming to disrupt and degrade the routing service have a serious impact on the overall operation of the entire network. In this paper we are going to go over the security attributes in wireless sensor networks. Attacks that commonly affect the sensor network routings can be classified and countered if one closely considers the attributes that are important in secure routings. In this paper, first we explain the goals of attackers that attack the wireless sensor networks and then, some important attributes of security mechanism will be shown. Finally we compare the protocols based on the main security attributes and application type. The organization of this report is as follows: In Section 2, the main characteristics of the routing. protocols in wireless sensor networks are discussed. Security goals are explained in Sections 3. Possible goals of attackers on attacking to routing protocols are discussed in Section 4. Security attributes and their effects on routing protocols are explained in Sections 5 and 6. Finally, conclusions are made in Section 7.

2. MAIN OBJECTIVES OF ROUTING PROTOCOLS

Wireless sensor networks have many restrictions. Limited energy supply, limited bandwidth of transceivers and computing power of nodes are some of these restrictions. In designing a WSN, carrying out data communication is a main goal while making efforts to prolong the lifetime of the network. In designing the routing protocols for WSN, the following key factors to be considered. These factors must be overcome before efficient communication can be accomplished [1], [3].

- ***Deployment of Nodes*****:** Depending on application, deployment of nodes is deterministic or randomized. In deterministic deployments the data is routed through predetermined paths whereas in randomized deployment is needed clustering to have connectivity and energy efficient operation.
- ***Energy Consumption*****:** Each node in WSN has a limited power supply, which is used both for computation, sending and routing the data. So malfunctioning of a sensor node due to lack of power can cause significant changes in topology of WSN and rerouting and reorganizing may be required.
- ***Data Reporting Model*****:** Data reporting in WSN can be categorized into time-driven, event-driven, query-driven and hybrid. Depending on the application, one of these models would be suitable. A for instance in application that data is monitored periodically; time-driven data reporting is a good prospect.
- ***Fault Tolerance*****:** In WSNs some nodes might fail or not have enough power to send or route their data. These faults should not affect the overall task of the network and WSN should be able to reorganize itself and use other routes to overcome these failures. So fault tolerant WSNs have to have some levels of redundancy.

• ***Scalability*:** In a WSN, over hundreds or thousands nodes may be deployed. Any routing protocol must be able to work with this number of nodes. It should be scalable to respond to events in the environment.
• ***Data Aggregation*:** In a WSN, nodes may produce similar data packets. These data can be aggregated to reduce number of transmissions. Some functions like min, max, average, and suppression can be used to aggregate data. This technique helps to energy efficiency and diminishing number of transmissions.
• ***Quality of Service (QOS)*:** Data in some WSNs should be transferred to a destination within a limited time otherwise they would be useless. In these applications, a bounded latency time is a condition to specify validity of data. In many other applications conserving energy has more priority than quality of data sent, so the routing protocol should consider the energy consumption and reduce the quality of service to prolong the lifetime.
• ***Security*:** Security is very important for many applications and even critical for some applications like military and homeland security [4]. A routing protocol should be resistive to several attacks. An attacker can easily inject some data to the network and operate like several nodes and route the data selectively. A routing protocol should consider security and guarantee the integrity, authenticity, and availability of messages in the presence of adversaries.

3. SECURITY IMPORTANCE

In the previous section we explained some important characteristics in sensor networks routing. In this section we are going to highlight one of the attributes, Security. Most of previous works on sensor network routing protocols assume a safe and secure environment where all sensor nodes cooperate with no attacker present. But we know that in real environment there are many attacks that can affect the performance of sensor networks routing. Attackers use different kinds of attacks to damage the sensor networks or listening and capturing important data. In the ideal world the security goal can be obtained when every node receives all messages intended for it and be able to verify the integrity of every message [3]. In this paper we will first explain the target of attackers and then will investigate some main factors in security of routing protocols based on this important goal. Finally we will compare the various kinds of routing protocols based on these attributes.

4. TARGET OF ATTACKERS

In this section we explain the possible objectives of attackers. Almost all the attackers have one of these major objectives from their attacks. Attackers usually use different methods to damage the networks. They use different kinds of attacks for their malicious goals and damage the whole or parts of networks using these attacks.

• ***Deleting important data and flow suppression*:** One of the possible methods for damaging networks is to penetrate in to the network as a node and then deleting or refusing to forward the information which is coming to this malicious node. With this method the other nodes in the network cannot obtain this specific information, which is eliminated with malicious node. Also attackers can suppress flow using the structure of routing or using different kinds of attacks. For example in directed diffusion an adversary can suppress the flow using negative reinforcements.
• ***Diverting routing traffics*:** Sometimes attackers put a compromised node which is especially attractive to surrounding nodes with respect to the routing algorithm in the network, and by using this attractive node try to lure all the traffic from a particular area through this compromised node. With this method the routing traffics of network change and it can damage the network.
• ***Listening to the transmission data and capturing important data*:** In some application of sensor networks like military application, protecting data from enemies are very important. In these situations, enemies and attackers try to drop important data. They usually put some malicious nodes in the network and then by advertising some alluring routes try to capture important data. In this method they convince the other nodes to send their information to these malicious nodes.
• ***Reducing the efficiency of the network*:** Sometimes attackers use different kinds of attacks to reduce the efficiency of the network. They usually use these techniques in front of fault-tolerant schemes to reduce their effectiveness.

5. ATTRIBUTES AND MAIN FACTORS OF SECURITY MECHANISM

In this section we will define the security attributes of routing protocols in wireless sensor networks which with them the attackers can not achieve their goals. Security attributes are the mechanisms that allow the routing protocols to defend against the possible threats in the whole network. These attributes consist of identity verification, bi- directionality confirmation, topology

structure restriction, base station decentralization and braided and multi-path transmission and are presented as follows:

1. *Identity check*: The identity of nodes, i.e., the characteristics of each and every node in wireless sensor networks should be checked from time to time by base stations or the gateways in each cluster.

2. *Bi-directionality Property*: Nodes in the networks should be checked for being bi-directional. This is because of the fact that nodes receiving a message from a neighbor should know that if the sender is a trusted sender or not, i.e., they should check whether the sender is in the range of their transmission in other words whether it can receive their limited range transmissions.

***3. Restriction on Topology*:** The structure of the topology in wireless sensor networks should not be able to expand randomly. This is done using strict rules initiated from the base station.

***4. Base Station Decentralization*:** The base station in the wireless sensor networks should not be the sink to every single message. This is mainly because of the fact that fake base stations created by the adversary can direct all the sources to themselves.

5.*Multi-PathTransmission*: Multi-path transmissions are needed especially when the probability of being compromised by the adversaries is high in sensor networks. This attribute calls for sending k messages instead of one, so that the attackers are defeated in selectively forwarding the messages.

6. COMPARISON OF ROUTING PROTOCOLS BASED ON SECURITY ATTRIBUTES

We are going to evaluate the attributes of the security schemes in this section. We take a close look at the characteristics of the attributes discussed in the previous section and evaluate their effects on routing protocols family. Also we will compare the groups of routing protocols based on their vulnerability to possible attacks according to these attributes. Finally, the routing protocols according to security attributes and possible attacks are tabulated. Some ad-hoc networks utilize public key cryptography for encryption or digital signature. This cannot be the case for our evaluation. This is because of the fact that public key cryptography is very expensive in terms of computation complexity and thus it is not preferred for resource constrained sensor networks. In our evaluation and comparison we focus on symmetric key cryptography as well as the attributes of secure routing protocols as follows:

***1. Identity check*:** In the mobile sensor networks, each and every node has a single specific identity, which is used for determining its characteristics such as its position or resource constraints. The identity of nodes has to be verified by the base stations in order to have a secure routing protocol. This is because of the fact that an attacker can easily compromise single or multiple nodes when strict identity check is not applied. Previously, the identity verification was possible if one used public key cryptography for digital signature. This is possible for networks that are not energy constrained. In this technique, a shared key and a secret key are used for identity verification. In sensor networks, however, we cannot use this type of verification. Our evaluations show that an attacker should only be able to take advantage of the identities that are already established, i.e., she cannot create new identities. Furthermore, the base station should limit the nodes surrounding each node for local communication. This restriction is essential, i.e., the nodes should not use any node except their previously verified neighbors. Based on this attribute, we have had a comprehensive evaluation of different families of protocols. Our study shows that two groups of protocols have the attribute of identity verification. Cluster based protocols and minimum cost forwarding family have the characteristic of verifying the identity of nodes. Not only it does prevent the outsider to attack the network, but also taking care of this attribute can have an efficient effect on removing the Sybil attacks. Let us have a closer look at the application types of protocols that are using identity verification in their structure. In terms of the application type, the algorithms that are based on efficiently forwarding packets from the source to sink using identifiers have the attribute of identity verification. These can be the protocols in which the nodes maintain the minimum cost required to reach the base station. Also, in those protocols that use cluster heads for efficiently disseminating queries such as low-energy adaptive clustering hierarchy, identity verification is used to prevent possible attacks.

***2. Bi-directionality property*:** In a network consisting of several nodes, messages are sent and received by thousands of links over the network. Our evaluations show that there is a strict need for confirming the property of being bi-directional for each and every link in the network. It is interesting that checking the bi-directionality of the links before performing the tasks wanted is equivalent to identity verification discussed in the previous attribute. This attribute is a sub-set of identity verification in the sense that when an identity in a network is verified, the attribute of being bi-directional is checked as well. Checking the links in the network for being bi-directional is done in the applications that are

using geographic and energy aware or greedy perimeter stateless routings. These applications consist of protocols in which identifying the nodes position is the main concern. Furthermore, when there is a need for matching the queries with data events with minimum cost using agents that are sent through the network, this attribute is considered because these agents have to be checked for having this specific attribute.

***3. Restriction on Topology*:** The structure of the topology in the sensor network should be restricted in terms of expansion or modification. Not only it is important because of the self-organizing nature of the network but it also poses an important security attribute called restriction on topology. If the topology is well structured, information such as the location of the nodes and the neighbors are easy to control by the base station. This also reduces the need for advertisement of IDs or time stamps by nodes because the exact topology is previously well known.

***4. Base Station Decentralization*:** In any kind of sensor network, there is a base station, which is the sink of all messages obtained through the network. We have taken a close look at this, and define an attribute called base station decentralizing. This attribute calls for a structure that is not initiated at base station. Instead, if localized interactions are used and network does its duty without initiation from the base station, this security attribute is taken into account. If a protocol pays attention to this attribute, private and out of bound channels are detected because the sink of the messages are not solely base stations. Moreover, in protocols that advertised information is not used to construct the topology this attribute is considered. Wormholes and sinkholes are easily protected using this attribute. For clarification, we have evaluated geographic protocols in which the topology is constructed on demand using localized interactions. The nodes, here notice these attacks because the distance between two nodes cannot be fake. The topologies that are based on energy conserving and those, which are cluster based, consider this attribute. This attribute is well utilized when sensor networks have to be deployed in hard to reach and unattended areas. Because of the power constrained nature of these networks; nodes have to be in several levels according to the power they consume. This important nature calls for localized algorithms in which the base station is not the initial starting source. Geographical routing protocols, directed diffusion multi path, energy conserving and cluster based protocols are built considering this attribute.

***5. Multi-path Transmission*:** In networks that a number of paths are used for message routing, this attribute is taken into account. Considering this attribute, the attacks that are based on selective forwarding are ineffective. In applications where energy conservation topologies are used, the transmission can be based on multi path routing. These applications can use this security attribute to affect the attacks that compromise the nodes to selectively forward the information. In applications that this attribute is not taken into account, either because of the resource constraints or because of the usage of a protocol that is not based on multi-path routing, participating nodes may be compromised and can not be trusted in forwarding received information. Considering the above-mentioned attributes Table 1 compares and evaluates the security mechanism. As you can see in this table, some of routing protocols such as directed single path diffusion have low security and are open to attacks but some of them like directed diffusion multi path are more secure and are mostly preserving against adversary attacks, but we can see that none of these protocols have all the security attributes and all of them are susceptible at least against one attack.

Table I

COMPARISON OF ROUTING PROTOCOLS BASED ON SECURITY FACTORS

Protocols	Main Attributes				
	Identity Check	Bi-directional Property	Restriction on Topology	Base Station Decentralization	Multi-path Transmission
Directed Diffusion multi path	No	Yes	Yes	Yes	Yes
Directed Diffusion single path	No	No	Yes	No	No
TinyOS Beaconing	No	No	Yes	No	No
Geographic Routing	No	Yes	Yes	Yes	No
Rumor Routing	No	Yes	Yes	No	No
Clustering Based Protocol	Yes	No	Yes	Yes	No
Energy conserving Topology Maintenance	No	No	Yes	Yes	Yes

7. CONCLUSION

Most of the previous works on sensor network routing protocols assume a safe and secure environment where all sensor nodes cooperate with no attacker present. However, in this paper we have found that recently proposed routing protocols for these networks do not

provide necessary security and are mostly open to attacks. In our paper, we found out that there is no routing protocol that satisfies our proposed security goals completely and all kinds of protocols have some loop holes based on which an adversary can attack them. Future work involves implementation of secured routing protocol, which satisfies all the security factors of secured routing in wireless sensor networking.

REFERENCES

[1] Jamal N. Al-Karaki, and Ahmed E. Kamal "Routing Techniques in Wireless Sensor Net- works: A Survey,"

[2] Gergely Acs, Levente Buttyan and Istvan Vajda, "Modelling adversaries and security objectives for routing protocols in wireless sensor networks," *Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks*, pp. 49-58, 2006.

[3] Chris Karlof, David Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *Proceedings of the IEEE International Workshop on Sensor Network Protocols andApplications*, pp. 113-127, May 2003.

[4] Du, X., and Lin, F. "Secure cell relay routing pro- tocol for sensor networks," Performance, Com- puting, and Communications Conference, 2005. IPCCC 2005, pp. 477-482, April 2005.

[5] Hamid, A., Mamun-Or-Rashid, Choong Seon Hong, "Defense against lap-top class attacker in wireless sensor network," *The 8th International Conference on Advanced Communication Technology*, vol.1, Feb. 2006.

[6] J. R. Douceur, "The Sybil Attack," *In 1st International Workshop on Peer-to-Peer Systems (IPTPS 02)*, March 2002.

[7] B. Chen, K. Jamieson, H. Balakrishnan, and R. Morris, "Span: An energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks," *ACM Wireless Networks Journal*, vol. 8, no. 5, September 2002.

[8] algorithm for mobile wireless networks," *In IEEE INFOCOM '97*, pp 1405-1413, 1997

[9] C. Intanagonwiwat, R. Govindan and D. Estrin, "Directed diffusion: A scalable and robust communication paradigm for sensor networks," *In Proceedings of the Sixth Annual International Conference on Mobile Computing and Networks (MobiCOM '00)*, August 2000.

[10] Wendi Rabiner Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan "Energy-efficient communication protocol for wireless microsensor networks," *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences*, Jan. 2000.

[11] Intrusion Detection for Routing Attacks in Sen- sor Networks Chong Eik Loo1 Mun Yong Ng1 Christopher Leckie2 Marimuthu Palaniswami

[12] Mohammad Nikjoo S, Arash Saber Tehrani and Priyantha Kumarawadu," Secure Routing in Sensor Network," *Proceedings of the 8th international IEEE conference in* 2007