Securing Ad-hoc On-Demand Distance Vector Protocol in Wireless Sensor Networks

Abstract

- Wireless sensor networks (WSNs) are considered to be one of the most important technologies of the 21st century. As a result, WSNs have been used in numerous applications in industry, health monitoring, environmental monitoring, and other related fields. However, the unprotected nature of WSN protocols such as the Ad-hoc On-Demand Distance Vector (AODV) Protocol makes them prone to malicious attacks. One such attack is the replay attack.
- A single sensor node has limited computation and communication capabilities, but processing routing information through data structures with acceptable time and space complexity can lead to secure data acquisition and sensing. Sensor nodes have limited energy resources, so this attack can have a serious impact on network functionality.

Existing system

- WSNs have been used in numerous applications in industry, health monitoring, environmental monitoring, and other related fields. However, the unprotected nature of WSN protocols such as the Ad-hoc On-Demand Distance Vector (AODV) Protocol makes them prone to malicious attacks.
- The more sophisticated the network, the wider the range of potential attacks that could be performed to sabotage the dedicated functionalities of that network. Replay attacks are among the most common and easily performed attacks.

Hardware requirement

Processor	-	Pentium –III
Speed	-	1.1 Ghz
RAM	-	256 MB(min)
Hard Disk	-	20 GB
Floppy Drive	-	1.44 MB
Key Board	-	Standard Windows Keyboard
Mouse	-	Two or Three Button Mouse
Monitor	-	SVGA

Software requirement

• Operating System	-	Windows 7/8
• Application Server	-	Tomcat 5.0
• Front End	-	JAVA
• IDE	-	NETBEANS 7.1
• Back-End	-	HEIDISQL 3.5

Proposed system

- WSNs are the result of advancements in the technology fields of micro-electro-mechanical systems (MEMS) and other related areas of research, such as communication networks and embedded systems.
- A low-cost, less power demanding, space efficient network structure is available for multiple uses and purposes .
- The field of WSNs is a fertile source of applications in industry, military, health practices, scientific research, and other sectors. Composed of inexpensive sensors triggered by the surrounding environment, WSNs can collect meaningful data, which can then be analyzed for deployment purposes.

- Replay attacks have an inevitable impact on energy storage in WSN nodes. They decrease residual energy and increase exchanged protocol and data messages. Bloom filters can salvage energy storages in different levels according to how big the WSN is and how long the path of transmission is.

Conclusion

- Data collected by sensor networks are basically what the sensor nodes detect. Sensor nodes, as illustrated in can detect light, heat, humidity, sound, weight, or any other measurable form of data that can be translated to parameter values according to what type of sensor network application is in use.

Reference

- [1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: a survey. *Computer Networks”*, *38*(4): 393–422. http://doi.org/10.1016/S1389-1286(01)00302-4, 2002
- [2] T. Aura, “Strategies against Replay Attacks”. *Proceedings of Computer Security Foundations Workshop,* 59–68. Rockport, MA: IEEE
 http://doi.org/10.1109/CSFW.1997.596787, 1997.
- [3] B. Bloom, “Space/Time Trade-Offs in Hash Coding with Allowable
 Errors”. *ACM Communications*, 13(7): 422—426, 1970.
- [4] A. Broder, and M. Mitzenmacher, “Network Applications of Bloom Filters: A Survey”. In *Internet Mathematics* 1(4): 485–509. A K Peters, Ltd. http://doi.org/10.1080/15427951.2004.10129096, 2004.