Asian Journal of Information Technology 15 (19): 3687-3692, 2016
ISSN: 1682-3915
© Medwell Journals, 2016

Performance of Security Algorithm Against Malicious Nodes Based Wireless Sensor Network

D. Hemanand and N. Sankar Ram
Anna University, 600025 Chennai, India

Abstract: Wireless Sensor Network (WSN) is being emerged as a prevailing technology in future due to its wide range of applications in military and civilian domains. These networks are easily prone to security attacks since these networks are deployed unattended and unprotected environment. Some of the inherent features like limited battery and low memory make sensor networks infeasible to use conventional security solutions which needs complex computations and high memory. There are lot of attacks on these networks which can be classified as routing attacks and data traffic attacks. Some of the routing attacks in sensor nodes are wormhole, black hole and selective forwarding attack.In a black hole attack,compromised node drops all the packets forwarding through it. Ad hoc On-demand Distance Vector routing (AODV) is a very popular routing algorithm. However, it is vulnerable to the well-known black hole attack where a malicious node falsely advertises good paths to a destination node during the route discovery process. In this project, a defense mechanism is presented against multiple black hole nodes in IEEE. 802.15.4 based wireless sensor networks. In last, performance (Throughput, PDR and End-to-End delay) of security algorithm against the black hole nodes is analyzed.

Key words: Security, algorithm, nodes, sensor, wireless

INTRODUCTION

In recent advances in Micro-Electro-Mechanical Systems (MEMS) and wireless communication technologies made it possible to build small devices that can run autonomously and be deployed in a large-scale, low power, inexpensive manner that is acceptable to many commercial and government users (Sheela *et al*., 2012). These devices can be used to form a new class of distributed networking, namely Wireless Sensor Networks (WSNs). Sensor network'configurations range from very flat with few command nodes denoted as base stations, sinks or cluster controllers to hierarchical nets consisting of multiple networks layered according to operational or technical requirements. The robustness and reliability of such networks have improved to the point that enabled their proliferation to a wide range of applications for a variety of tasks from battlefield surveillance and reconnaissance to other risk-associated applications such as environmental monitoring and industrial controls.Since the early 1990s, distributed sensor networking has been an area of active research. The trend is to move from a centralized, super reliable single-node platform to a dense and distributed multitude of cheap, lightweight and potentially individually unreliable components that as a group are capable of far more complex tasks than any single super node. The intuition is to have individual sensor nodes share information with each other and collaborate to improve detection probabilities while reducing the likelihood of false alarms. Research prototype sensors (UCB motes), Tmote Sky, Telos, Eyes IFX, Scatter Web MSB-430 are designed and manufactured, energy efficient MAC, topology contro protocols and routing schemes are implemented and evaluated, various enabling technologies such as time synchronization, localization and tracking are being studied and invented. All these provide sensor networks tremendous potential for information collection and processing in a variety of application domains (Biswas and Ali, 2007). The first generation of sensor nodes facilitated the genesis of wireless sensor networks as they exist today, small resource-constrained embedded devices that communicate via low-power, low-bandwidth radio, capable of performing simple sensing tasks . A first set of scenarios for thesenetworks included stationary nodes sensing ephemeral features of the environment, like temperature, noise, air pollution, etc. By continuously monitoring these surrounding attributes, they solved relatively small scale specialized problems such as forest monitoring, preventative maintenance, etc.,

Corresponding Author: D. Hemanand, Anna University, 600025 Chennai, India

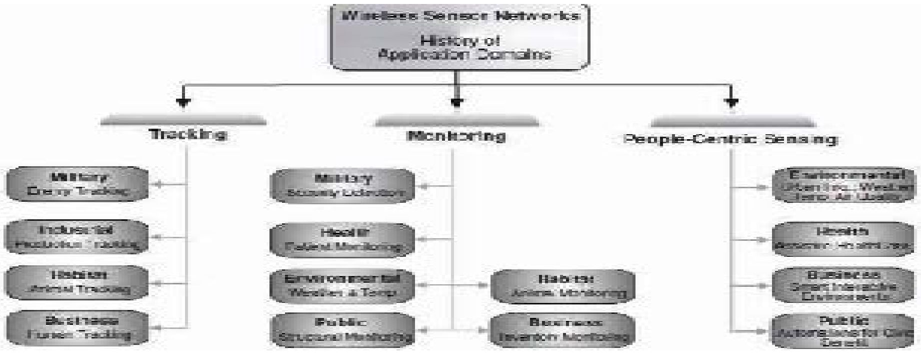

Fig. 1: History of research in sensor networks application domain

Table 1: Traditional sensor networks vs. People-centric sensing

Traditional Sensor networks	People-centric sensing
Specially designed deployed hardware	Leveraging available devices
Fully automatic and standalone systems	Humans in the loop
Thousands of small devices	Systems of heterogeneous devices
Fixed, static deployment	Mobility

as shown in Fig. 1. Early sensor networks as shown in Table 1, functioned primarily into two important application domains: monitoring and tracking. WSNs can be configured to monitor a variety of target types (Lu *et al*., 2009). The networks themselves are mode-agnostic, enabling multiple types of sensors to be employed, depending on operational requirements; cameras as vision sensors, microphones as audio sensors, ultrasonic, infrared, light, temperature, pressure/force, vibration, radio activity, seismic sensors and so on (Mahajan *et al*., 2008).

Target tracking can also be performed effectively with sensors deployed as a three-dimensional field and covering a large geographic area. Therefore, some of the most common applications are military, medical, environmental and habitat monitoring industrial and infrastructure protection ,disaster detection and recovery, green growth and agriculture, intelligent buildings, law enforcement, transportation and space discovery. For instance, in enterprise scale manufacturing and retail companies, sensor networks can be combined with RFID (Radio Frequency ID) tags to monitor inventory and support in-process parts tracking. These networks can automatically report problems at various stages such as in plant manufacturing, packaging and equipment maintenance (Papadimitratos and Haas, 2003).

In this study, monitoring is the main application area of the sensor networks. But, due to black hole attack the packets are dropped due to which some of the monitored data is lost. These may degrade the performance of our application. For example, in military battle field; if we lost the data about enemy tanks arrival, then we would lost the battle. It concerns about security issues on WSN routing protocols, particularly on black hole attacks which prevent the data from reaching the end points (sinks). This type of attacks is most challenging to detect and avoid. This study, focuses on the effects of black hole attack on AODV routing protocols in WSNs.

MATERIALS AND METHODS

In WSN, sensor nodes use wireless communication to send packets. Due to limited transmission range, a sensor node uses multi hop transmission to deliver the packet to a base station. Hence a packet is forwarded through so many nodes to reach the destination. Sensor networks are usually deployed in hostile environment where an adversary can compromise some internal nodes which may launch various inside attacks. One kind of attack caused by malicious nodes is Black hole (Karlof *et al*., 2004).

The black hole attack is one of the simplest routing attacks in WSNs. In a black hole attack, the attacker swallows (i.e., receives but does not forward)all the messages it receives, just as a black hole absorbing everything passing by. But refusing to forward any message it receives, the attacker will affect all the traffic flowing through it. Hence, the throughput of a subset of nodes, especially the neighboring nodes around the attacker and with traffic through it is dramatically decreased. Different locations of the attacker induce different influences on the network. If the attacker is located close to the base station, all the traffic going to the base station might need to go through the attacker. Obviously, black hole attacks in this case can break the communication between the base station and the rest of the WSN and effectively prevent the WSN from serving its purposes. In contrast, if a black hole attacking node is at the edge of the WSN, probably very few sensors need it to communicate with others. Therefore, the harm can be

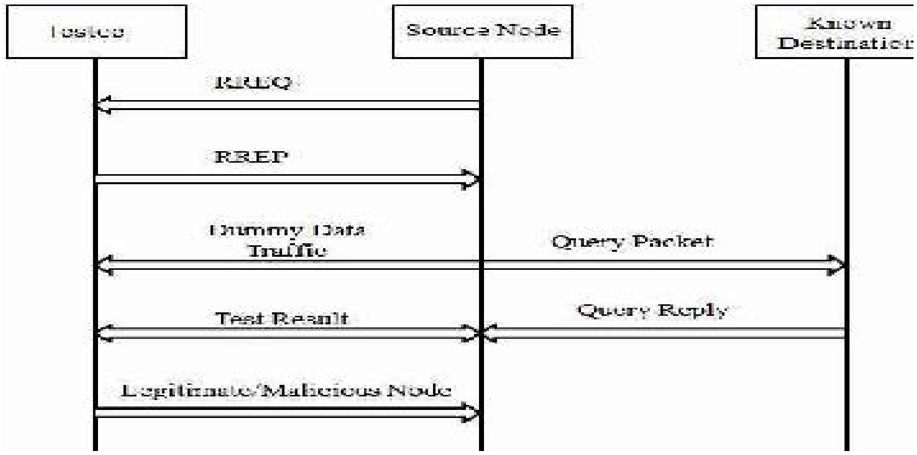

Fig. 2: Black hole detection

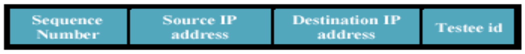

Fig. 3: Query packet

Table 2: Description of fields in query packet

Sequence number	The sequence number is the sequence number of the packet that it receives from the source
Source IP address	The source IP address is the address of the MR
Destination IP address	The destination IP address is the address of the known destination
Testee ID	The testee ID is the source IPaddress of the testee evaluated

very limited (Krontiris *et al*., 2007; Traynor *et al*., 2006). Attackers can use different types of devices to attack the targeted network these devices have different computation power, radio antenna and other capabilities. Two common categories have been identified by Karlof and Wagner including laptop-class and mote-class attackers. Laptop class attackers may possess powerful hardware such as faster CPU, larger battery and high-power radio transmitter. This hardware allows a more broad range of attacks which are more difficult to stop. Their goal may be to run some malicious code and seek to steal secrets from the sensor network or disrupt its normal functions. For example, in the authors demonstrate how to extract cryptographic keys from a sensor node using a JTAG programmer interface in a matter of seconds.

Proposed scheme: The proposed block diagram of black hole detection is shown in Fig. 2 and it follows: The source node sends an RREQ packet to the testee. The destination address is that of a randomly chosen known destination. It assumes that the source node is already aware of a route to the destination and issues an exclusive RREQ to determine the validity of the nodes in its neighborhood. The 'testee' sends an RREP packet back to the source. This RREP could be a valid or a spurious one. A malicious 'testee' would include a spurious RREP with a high sequence number and a low hop count value. On the other hand, a valid testee would generate RREP only if it is aware of a route to this destination.

Next, the source nodes end a testee data packet and forward it to the 'testee'. The testee packet is like any other regular data packet. However, its payload is masked and padded with a random data stream. The Source sends a "Query packet" (Fig. 3 and Table 2) to the destination to inquire about the packet that it forwarded to the 'testee ' in Step 3. The feedback module uses the alternate path table to retrieve the known alternate route to the chosen destination. It then routes the query packet through this route. The various fields in the query packet consist of the sequence number, Source IP address, Destination IP address and the testee id.

The source IP address is stamped with the address of the node and the destination IP address is that of the chosen destination. It also consists of a testee id field that is the source IP address of the testee which is being evaluated. When the destination receives such a trace query, it processes it by examining its most recently received traffic cache. This cache captures the most recently received traffic from different sources including the source ids, the timestamp when it was received and the count of the number of packets received from this source.

If the destination finds the testee id in its traffic cache, it prepares a "Query reply packet", the destination address of which is equal to the source address of the source from which the query packet came. The query reply packet also includes the following data in its information field: the count of the number of packets received and the timestamp of the last received packet. Thus, the Query reply packet is unicast to the source using the same route by which the trace packet came.

When the source node receives the query packet, it hands it to the feedback module. Depending on the content of the information field, the integrity of the testee is determined. If the packet has been received at the destination, the 'testee' is considered to be a "Good MR". If the field is empty, then the 'testee ' is considered a malicious attacker.

RESULTS AND DISCUSSION

For Simulation, we set the parameter as shown in Fig. 2. The simulation is done by using network simulator 2.35 to analyze the performance of the network by varying the no. of nodes and terrain size. The metrics used to evaluate the performance are given below.

Packet delivery ratio: It is defined as ratio between the number of packet generated by the "application layer "CBR sources and the number of the packets received by the CBR sinks at the final destination.

Average end-to-end delay: This is the average delay between the sending of the packet by the CBR source and its receipt at the corresponding CBR receiver. This includes all the delays caused during route acquisition, buffering and processing at intermediate nodes, retransmission delays at the MAC layer etc. It is measured in milliseconds.

Throughput: It is measure of total data transferred from CBR source to CBR destination in a given time. It is measures in Kilobits per second. The evaluation was done by analyzing the performance result of following conditions:

- Using normal AODV protocol (without attack) and
- Using AODV protocol with malicious nodes (with attack)
- Using SAODV protocol with malicious node (with security algorithm)

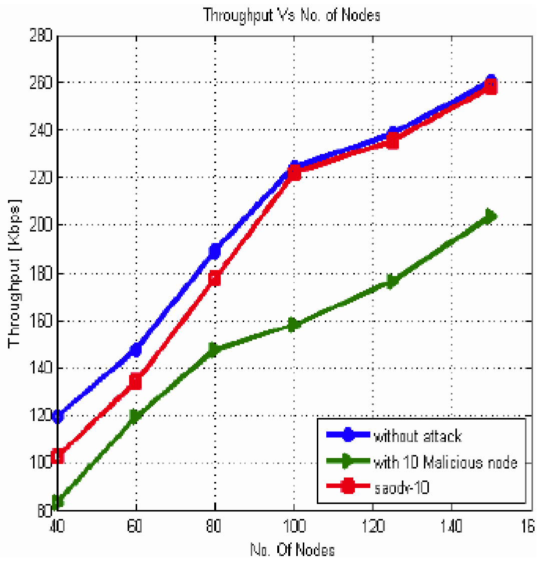

Fig. 4: Analysis of throughput for fixed terrain size

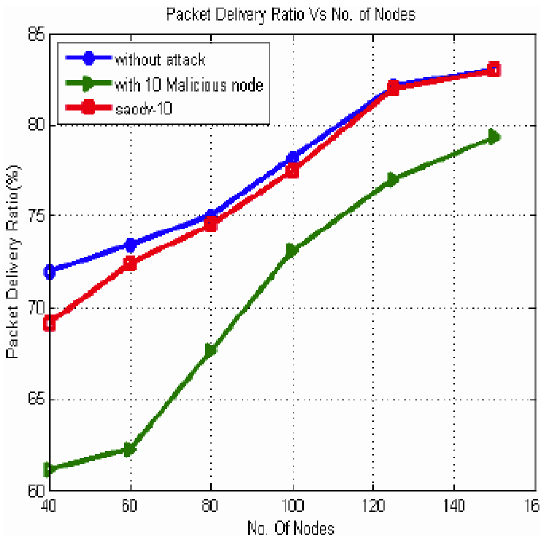

Fig. 5: Analysis of packet delivery ratio for fixed terrain size

Figure 4 shows that AODV outperform AODV with black hole attack when compare throughput. In case of AODV with black hole attack, throughput increases as number of node increases. As nodes increases hops in the network gets reduced. This leads to performance up gradation in the network. The Security Algorithm (SAODV) shows very close result to AODV without attack scenario. As number of nodes increases the security algorithm outperforms compare to less numbers of node in the network. The reason is as numbers of nodes increases in the networks it creates new paths from source to destination it leads more possibility of delivering of data to its destination.

In AODV protocol if many nodes are sending and receiving data traffic simultaneously placing more malicious node uniformly causes severe damage. It increases the probability of route affected malicious node. As shown in Fig. 5 when there is no malicious node

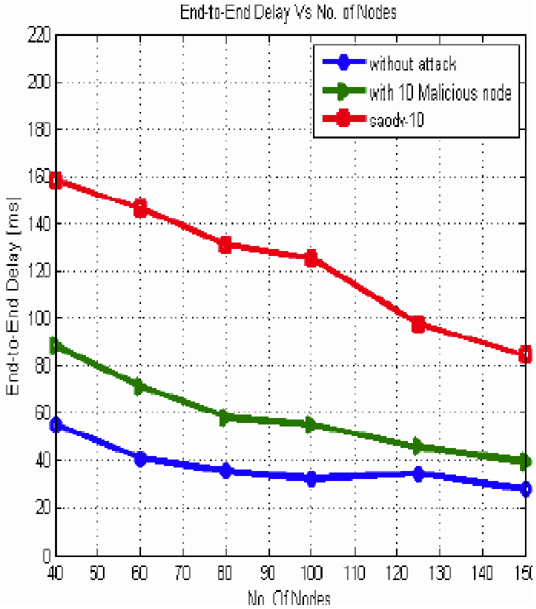

Fig. 6: Analysis of average end-to-end delay for fixed terrain size

packet delivery ratio is more. It increases as numbers of node increases from approximately 72-83% but packet delivery ratio decreases as the malicious node added to the scenario.

The reason for degradation of PDR after placing the black hole node is that it simply absorbs the packet that comes in between the source and destination. So AODV with black hole attack has less packet delivery ratio than AODV without black hole attack. While incorporating security algorithm in the presence of malicious nodes the packet delivery ratio approaching to the line for without attack. As numbers of nodes increases in the network security algorithm perform well due to the reason mentioned above for the throughput.

From Fig. 6 shows delay of AODV with and without black hole attack and SAODV. In case of SAODV in the presence of black hole attack delay suddenly increases as alternative chosen path have more number of hops count.

CONCLUSION

Wireless sensor networks have emerged as an important new area in wireless technology. In the near future, the wireless sensor networks are expected to consist of thousands of inexpensive nodes. Each node has sensing capability with limited computational communication power. It enables us to deploy a large-scale sensor network. Security in wireless sensor network is vital acceptance and can be used in networks for secure communication. In particular, wireless sensor network product in industry will not get acceptance unless there is a full proof security to the network. In this project performance analysis of malicious node in wireless sensor node is carried out.

In the performance evaluation of proposed security algorithm against black hole attack is simulated by varying number of nodes; Terrain size and number of black hole nodes. Performance metrics like throughput, packet delivery ratio and average end-to-end delay are measured. From the results it is evaluated that packet delivery ratio and throughput gets decreased as number of malicious node increases. For both cases its average end-to-end delay increases.

REFERENCES

Biswas, K. and M.L. Ali, 2007. Security threats in mobile Ad hoc network. Master's Thesis, Department of Interaction and System Design, School of Engineering Blekinge Institute of Technology, Sweden.

Karlof, C., N. Sastry and D. Wagner, 2004. TinySec: A link layer security architecture for wireless sensor networks. Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, November 3-5, 2004, Baltimore, MD., USA., pp: 162-175.

Krontiris, I., T. Dimitriou, T. and M. Mpasoukos, 2007. Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks. In: Algorithmic Aspects of Wireless Sensor Networks. Miroslaw, K., J. Cichon and K. Przemyslaw (Eds.). Springer, Berlin, Germany, ISBN:978-3-540-77870-7, pp: 150-161.

Lu, S., L. Li, K.Y. Lam and L. Jia, 2009. SAODV: A MANET routing protocol that can withstand black hole attack. Proceedings of the International Conference on Computational Intelligence and Security, Volume 2, December 11-14, 2009, Beijing, China, pp: 421-425.

Mahajan, V., M. Natu and A. Sethi, 2008. Analysis of wormhole intrusion attacks in MANETS. Proceedings of the IEEE Conference on Military Communications MILCOM-2008, November 16-19, 2008, IEEE, Newark, Delaware, ISBN: 978-1-4244-2676-8, pp: 1-7.

Papadimitratos, P. and Z.J. Haas, 2003. Secure message transmission in mobile ad hoc networks. Ad Hoc Netw., 1: 193-209.

Sheela, D., V.R. Srividhya, B. Asthma, Anjali and G.M. Chidanand, 2012. Detecting black hole attack in wireless sensor network sing mobile agent. Proceedings of International Conference on Artificial Intelligence and Embedded Systems, July 15-16, 2012, AMC Engineering College, Bangalore, India, pp: 45-48.

Traynor, P., H. Choi, G. Cao, S. Zhu and T. Porta, 2006. Establishing pair-wise keys in heterogeneous sensor networks. Proceedings of the 25th IEEE International Conference on Computer Communications, April 23-29, 2006, Barcelona, Spain, pp: 1-12.

Xing, K., S.S.R. Srinivasan, M. Jose, J. Li and X. Cheng, 2010. Attacks and Countermeasures in Sensor Networks: A Survey. In: Network Security, Scott, C.H.H., D. MacCallum and Z.D. Ding (Eds.). Springer, Berlin, Germany, ISBN:978-0-387-73820-8, pp: 251-272.