Journal of Engineering and Applied Sciences 12 (Special Issue 2): 6286-6290, 2017
ISSN: 1816-949X


# Quality of Service and Angle Based Adversary Detection Scheme (QADS) for Wireless Sensor Networks

K. Sudhaman, M. Anand and M. Janakirani
Department of Electronics and Communication Engineering,
M.G.R Educational and Research Institute University, 600095 Chennai, India

**Abstract:** Individual nodes of a Wireless Sensor Network (WSN) could be easily compromised by the adversary due to the constraints such as limited battery lifetime, memory space and computing capability deployed in a hostile environment. It is critical to detect and isolate the compromised nodes in order to avoid being misled by the falsified information injected by the adversary through compromised nodes. There are large numbers of studys that describe the adversary detection scheme in wireless sensor networks. Each study has its own disadvantages. In this study, a Quality of Service (QoS) and Angle based adversary detection scheme is proposed for wireless sensor networks. Simulation results show that the proposed QADS scheme is better compared to the existing scheme.

**Key words:** Wireless Sensor networks, Quality of Service, adversary node, proposed, scheme, compared, angle, routing

## INTRODUCTION

Wireless Sensor Network (WSN) is composed of a large number of small devices with limited power, processing and communication capabilities which are densely deployed inside a phenomenon. Sensor nodes have two main functionalities: monitor the environment and send the sensed data to a special node, called the sink. Sensor nodes can send the monitored data periodically or when an event occurs. Some applications need a mixture of both periodic and event-based data reporting.

The ability of the sensor nodes in a WSN may vary widely. For example, a simple sensor node may monitor a single physical phenomenon while a more complex device may combine lots of sensing techniques to monitor and operate. The presently available sensor nodes lack hardware support for tamper-resistance and hence they are vulnerable to various types of attacks by an adversary. In this case, each sensor node monitors the environment and besides sending periodical measurements to the sink, it also informs the sink when a specific event occurs.

In this study, the threshold value is taken into consideration form the QoS parameters and the node is decided whether it is a normal or a abnormal node. Simulation analysis shows that the proposed system shows better in terms of adversary node detection compared to the existing work. Usually, sensor nodes employ omni-directional antennas for wireless communication due to a variety of reasons including their small size, low cost, ease of deployment and simplified.

**Literature review:** The framework provides an appropriate abstraction of application specific detection mechanisms and models the unique properties of sensor networks. Based on the framework, alert reasoning algorithms are developed to identify compromised nodes (Zhang *et al*., 2008). Localized multicast for detecting node replication attacks evaluates the performance and security for both theoretically and via simulation. The probability of detecting node replicas is much higher than that achieved in previous distributed protocols (Zhu *et al*., 2007).

An attacker may not be able to precisely deploy the compromised sensors back into their original positions. The detection of location change will become an indication of a potential node compromise (Song *et al*., 2007). A routing mechanism transforms any shortest path routing protocol into a new protocol that does not create congested areas, does not have the associated security-related issues and does not encourage selfish positioning. Moreover, the network is more energy efficient than the same network using the original routing protocol and dies more gracefully (Mei and Stefa, 2008).

A Polynomial based Space-time related Pairwise key Predistribution scheme (PSPP) was designed in which the keying material of a node can only works at its initial

**Corresponding Author:** K. Sudhaman, Department of Electronics and Communication Engineering,
Dr. M.G.R Educational and Research Institute University, 600095 Chennai, India

deployment location (Fu *et al*., 2007). Randomized multicast distributes node location information to randomly-selected witnesses, exploiting the birthday paradox to detect replicated nodes while line-selected multicast uses the topology of the network to detect replication (Parno *et al*., 2005). Both algorithms provide globally-aware, distributed node-replica detection and line-selected multicast displays particularly strong performance characteristics.

A novel mobile replica detection scheme based on the Sequential Probability Ratio Test (SPRT) use the fact that an uncompromised mobile node should never move at speeds in excess of the system-configured maximum speed (Ho *et al*., 2008). A scheme was designed for detecting clone attacks in sensor networks which computes for each sensor a social fingerprint by extracting the neighborhood characteristics and verifies the legitimacy of the originator for each message by checking the enclosed fingerprint. The fingerprint generation is based on the super imposed s-disjunct code which incurs a very light communication and computation overhead (Xing *et al*., 2008).

A novel scheme based on weighted-trust evaluation to detect malicious nodes was proposed. The hierarchical network can reduce the communication overhead between sensor nodes by utilizing clustered topology (Atakli *et al*., 2008). Through intensive simulation, we verified the correctness and efficiency of our detection scheme. An Adaptive Early Node Compromise (AENC) detection scheme facilitates node compromise attack detection in a cluster-based WSN. The scheme was designed to achieve a low false positive ratio in the presence of various levels of message loss ratios. To achieve this feature, two ideas are used in the design. The first is to use cluster-based collective decision making to detect node compromises (Al-Riyami *et al*., 2016). The second is to dynamically adjust the rate of notification message transmissions in response to the message loss ratio in the sender's neighborhood.

## MATERIALS AND METHODS

**QoS and angle based adversary detection scheme:** WSNs are assumed as homogeneous, symmetric and static. In particular, the radio transceivers of all members of the network operate under the same configuration throughout the lifetime of the network. All nodes are uniquely identified and know their own geographical position which can be obtained using a positioning system. The value of a node's geographical position as well as its identifier is included in each of the messages it sends. It is assumed that message exchanges in the network are protected against tampering.

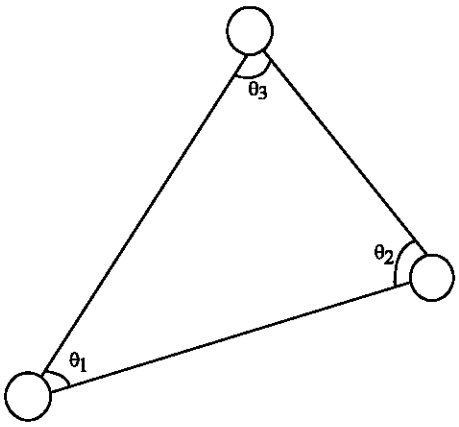


Fig. 1: Angle formation

In this study, QoS and Angle based Adversary Detection Scheme (QADS) is proposed. Adversary nodes are a peculiar type of attacks in which a node makes itself attractive to all other nodes with an intention to draw the entire traffic towards itself. The detection of adversary node is a very challenging task as it has almost every feature similar to that of other normal nodes.

Figure 1 shows that the source A, next hop B and closest neighbor node C forms a triangle. Where, $\theta_1$, $\theta_2$ and $\theta_3$ are three interior angles. Mathematically, the addition of all three node angles is 180°:

$$\theta_1+\theta_2+\theta_3 = 180° \quad (1)$$

If the sum of the angles in Eq. 1 adds up to make 180°, then the nodes are proved to be legitimate nodes. Otherwise, one among the three nodes forming the triangle is said to be faulty. The angle $\theta$ will be calculated by:

$$\text{Angle} = \text{Atan}2(dy, dx)\times\frac{180}{\pi} \quad (2)$$

$$dx = x_s - x_a$$

$$dy = y_s - y_a$$

In a triangle, the three neighbor angles add to 180°. If the node location is true, so that node is normal node otherwise the node is malicious.

Figure 2 shows that the computation of QoS in WSNs. The steps that are computed for QoS and angle based adversary detection scheme are included as follows: initially source sends route request to all its neighbors. The nearby nodes in the network receive the route request and sends back route reply messages back to the source node. Then the source calculates the neighbor node angle value. If the source gets the angle

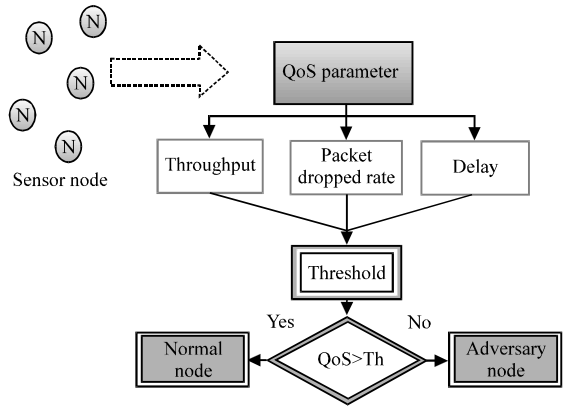


Fig. 2: QoS calculation

value 180, then the source compute the QoS parameters of that node. The QoS parameters include throughput, packet dropped rate and delay. The second step is to dynamically estimate the Threshold (Th) for the Maximum possible QoS in the network. Threshold value determines the overall QoS in the network, then each nodes QoS value are compared with the value 'Th'. If the node's QoS value is higher than the threshold, then that node is marked as an adversary node. Other nodes can be a normal node. The algorithm of QADS scheme explanation is given.

**Algorithm 1; QADS scheme:**

Step 1: Start
Step 2: Initialize the route discovery
Step 3: Calculate neighbour angle computation
Step 4: $\theta_1+\theta_2+\theta_3 = 180°$
Step 5: Estimate throughput, packet drop and delay for all nodes simultaneously
Step 6: Calculate threshold value using the equation:

$$Th = 3X-(Y+Z)$$

Where:
X-> Throughput
Y-> Packet drop
Z-> Delay

Step 7: If Qos is greater than the threshold value then the node is normal node. Otherwise the node is called as adversary node
Step 8: Stop

## RESULTS AND DISCUSSION

**Performance evaluation:** Evaluation of the protocols QADS and AENC is achieved using simulations in the network simulator. Such simulations use the common parameters indicated in Table 1. Performance evaluation of the QADS, AENC protocols are provided by estimating the packet delivery rate, packet loss rate, delay rate, Throughput, residual energy and routing overhead in the network.

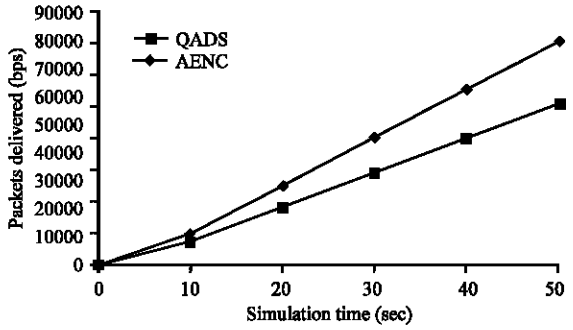


Fig. 3: Packet delivery rate

Table 1: Simulation parameters of QADS

| Parameters | Values |
|---|---|
| Channel type | Wireless channel |
| Radio propagation model | Tworay ground |
| Network interface type | Wireless Phy |
| Antenna type | Omni antenna |
| MAC type | 802.11 |
| Simulation time | 50 sec |
| Number of nodes | 50 |
| Transmission range | 250 m |
| Traffic model | CBR |
| Simulation area | 700×700 |

**Packet Delivery Rate (PDR):** The packet delivery rate is defined as the ratio of total data packets received by the destination to total send packets by source multiplied with number of receivers. The PDR is calculated by Eq. 3:

$$PDR = \frac{\text{Total Pack Received}}{\text{Total Pack Send}} \quad (3)$$

Figure 3, the proposed protocol QADS that increases the packet delivery rate compared to the existing protocol AENC. In QADS, transmit the data through the reliable routing path as a result increase the PDR but AENC decreases PDR because of it transmit the data through the unreliable path.

**Packet Loss Ratio (PLR):** The Packet Loss Rate (PLR) is the ratio of the number of packets dropped to the number of data packets sent. The PLR is calculated by Eq. 4:

$$PLR = \frac{\text{Total Pack Dropped}}{\text{Total Pack Send}} \quad (4)$$

Figure 4 indicates the packet loss rate of the proposed protocol QADS is lesser than the AENC protocol showing the efficiency of the QADS.

**Delay:** Delay is defined as the average time that a packet takes to transmit the network from source to destination. It is measured by Eq. 5:

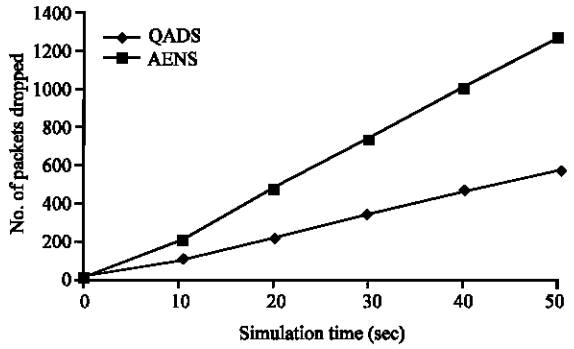


Fig. 4: Packet loss rate

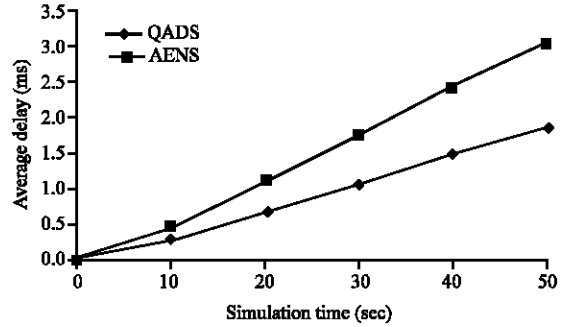


Fig. 5: Delay

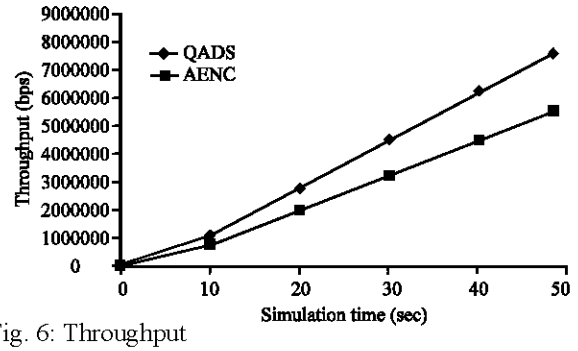


Fig. 6: Throughput

$$\text{Delay} = \frac{\text{Pack Received Time-Pack Sent Time}}{\text{Time}} \quad (5)$$

Figure 5 demonstrates that the delay of QADS and AENC. The average delay of the AENC is larger than the QADS indicating the improved performance of the QADS protocol.

**Throughput:** Figure 6 shows the performance of throughput of QADS and AENC protocols. The throughput of AENC is lesser than the QADS. It represents the increase in efficiency of the QADS protocol in the network. The throughput Eq. 6 is calculated as:

$$\text{Throughput} = \frac{\sum_0^n \text{Pkts Received (n)} \times \text{Pkt Size}}{1000}$$

## CONCLUSION

Quality of Service and Angle based Adversary Detection Scheme (QADS) for wireless sensor networks is proposed in this study. The threshold value is taken into consideration form the QoS parameters and the node is decided whether it is a normal or an adversary node. Simulation analysis shows that the proposed system shows better in terms of adversary node detection compared to the existing research.

## REFERENCES

Al-Riyami, A., N. Zhang and J. Keane, 2016. An adaptive early node compromise detection scheme for hierarchical WSNS. IEEE. Access, 4: 4183-4206.

Atakli, I.M., H. Hu, Y. Chen, W.S. Ku and Z. Su, 2008. Malicious node detection in wireless sensor networks using weighted trust evaluation. Proceedings of the Spring Simulation Multiconference, April 14-17, 2008, Ottawa, Canada, pp: 836-834.

Fu, F., J. Liu and X. Yin, 2007. Space-time related pairwise key predistribution scheme for wireless sensor networks. Proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing (WiCom 2007), September 21-25, 2007, IEEE, Shanghai, China, ISBN:1-4244-1311-7, pp: 2692-2696.

Ho, J.W., M. Wright and S.K. Das, 2008. Fast detection of node replication attacks in mobile sensor networks. Proceedings of the 16th IEEE International Conference on Network Protocols, October 19-22, 2008, IEEE, Orlando, Florida, USA., ISBN:978-1-4244-2506-8, pp: 308-317.

Mei, A. and J. Stefa, 2008. Routing in outer space: Fair traffic load in multi-hop wireless networks. Proceedings of the 9th ACM International Symposium on Mobile Ad-Hoc Networking and Computing, May 26-30, 2008, ACM, Hong Kong, China, pp: 23-32.

Parno, B., A. Perrig and V. Gligor, 2005. Distributed detection of node replication attacks in sensor networks. Proceedings of the IEEE Symposium on Security and Privacy, May 8-11, 2005, Oakland, CA., USA., pp: 49-63.

Song, H., L. Xie, S. Zhu and G. Cao, 2007. Sensor node compromise detection: The location perspective. Proceedings of the 2007 International Conference on Wireless Communications and Mobile Computing, August 12-16, 2007, ACM, Honolulu, Hawaii, ISBN:978-1-59593-695-0, pp: 242-247.

Xing, K., F. Liu, X. Cheng and D.H.C. Du, 2008. Real-time detection of clone attacks in wireless sensor networks. Proceedings of the 28th International Conference on a Distributed Computing System, June 17-20, 2008, Beijing, China, pp: 3-10.

Zhang, Q., T. Yu and P. Ning, 2008. A framework for identifying compromised nodes in wireless sensor networks. ACM Trans. Inform. Syst. Secur., Vol. 11 10.1145/1341731.1341733

Zhu, B., V.G.K. Addada, S. Setia, S. Jajodia and S. Roy, 2007. Efficient distributed detection of node replication attacks in sensor networks. Proceedings of the 23rd Annual Conference on Computer Security Applications, December 10-14, 2007, IEEE, Miami Beach, Florida, ISBN:0-7695-3060-5, pp: 257-267.