ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department Of CSE, JayaShriram Group Of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Enhanced Detection of Packet Droppers And Modifiers In Wireless Sensor Networks

R. Karthikeyan

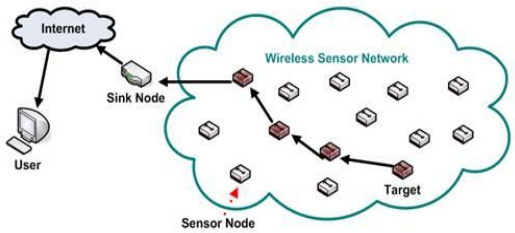
Department of Computer Science and Engineering, Sri Krishna College of Engineering and Technology, Coimbatore, Tamil Nadu, India

ABSTRACT- There are several emerging trends in the field of networks, out of which Wireless Sensor Networks(WSN) are gaining importance recent years due to its impact on Cost, ability to cope up with node and communication failures, Mobility, Capability to withstand harsh environmental condition, monitoring purpose and Ease of use. Despite Sensor nodes large collection of benefits there are few constrains such as Security, Quality of Service and Resource constrains which act as hurdle in implementing sensor network application in real world environment. Security is considered to be a critical parameter in Sensor network due to the fact that they are mostly deployed in an environment where human interaction is less. An opponent or intruder is one who may perform various attacks on packets in order to make a node compromise and cut short the communication to take place. Attacks that have been concentrated here are packet dropping and modification. Sensor applications are time critical and if compromised nodes are not detected, large quantities of irrelevant data can be injected into the network which in turn will have a greater impact on computational cost and storage overhead. In this paper Node Categorization and Heuristic Ranking (NCHR) is used along with our proposed scheme of energy consumption and delay aspects to identify compromised nodes and further a Secure Routing and Encryption techniques are provided to ensure reliable communication.

Keywords: Wireless Sensor Network, Packet Droppers, Packet Modifiers, Message Authentication Code, Compromised nodes, Routing.

I . INTRODUCTION

Wireless Sensor networks consist of large number of small sensor nodes having few constrains such as physical resource, limited computation capacity, restricted memory space and security. Sensor nodes are suitable with an onboard processor. Instead of sending the raw data to the nodes responsible for the fusion, they use their processing abilities to locally carry out simple computations and transmit the processed data.



A WSN consist of tiny devices which can monitor physical or environmental conditions such as temperature, sound, pressure, motion or pollutants etc. based on their area of interest and in turn produces data. These sensed data are further forwarded to the sink (gateway, base station, and user). A sensor network is often deployed in an

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department Of CSE, JayaShriram Group Of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

environment where human interaction is less to perform the monitoring and data collection tasks. Deploying in such an environment may result in lack of physical protection and leads to node compromising. Once nodes are compromised in WSN an opponent may come up with several attacks which are passive or active in nature to disrupt the communication. This paper deals with packets dropping and modifying packets which are common attacks that may be aroused by an opponent.

In this paper, a modified and simple yet effective scheme is proposed to catch both packet droppers and modifiers. In this scheme, first a routing tree is rooted at the sink. The sensor data are transmitted along the tree structure toward the sink, each packet sender or forwarder adds a small number of extra bits, which is called packet marks to the packet. The format of the small packet marks is intentionally designed such that the sink can obtain very useful information from the marks. Specifically, based on the packet marks, the sink can figure out the dropping ratio associated with every sensor node. Every participating node computes two MACs over the event, one using its key shared with the BS, and the other using its pair wise key shared with its upper associated node. The node transmits the packet along with the MAC value produced and the forwarding node verifies the data integrity. Then the sink runs node categorization algorithm to identify nodes that are droppers/modifiers for sure or are suspicious droppers/modifiers. As the tree structure dynamically changes every time interval, behaviours of sensor nodes can be observed in large variety of scenarios. Finally, as the information of node behaviours has been accumulated, the sink periodically runs the heuristic ranking algorithms to identify most likely bad nodes with small false positive. After finding out the compromised node secured routing path is found. A route request is broadcasted to all nodes which consist of a record listing the addressing of the intermediate nodes excluding the compromised nodes identified. Later shortest path is identified and data is transferred The proposed scheme is effective in identifying both packet droppers and modifiers with low communication and energy overheads and being compatible with existing false packet filtering schemes, that can be deployed together with existing false packet filtering schemes is detected.

II . RELATED WORKS

There are several approaches made for detection of vulnerable attacks. [2][3][4][5][6] Deals with packet dropping. [2] Detection of packet dropping attacks for WSN proposes a solution to identify paths that drop packets by using alternate paths, but it succeeds only when the alternate path does not have any malicious nodes. [3] In this scheme single path data forwarding is employed and later it is convertor in multipath data forwarding. [4][5][6] are related to routing process and neighbour monitoring mechanism. [7][8][9] Deals with packet modification. [7] In this SEF detect and filters out false reports based on probabilistic key distribution. [9] Proposes Location Based Resilient security to filter out packets, but in spite of all filtering techniques intruders are able to move on and communication overhead is increased. [10] Probabilistic Nested marking is proposed to locate vulnerable nodes and it does so within the framework of packet marking, but the evidence to find packet modifiers are also filtered out. [11] In this paper extensions to Dynamic Source Routing are given such as watchdog and pathrater. Watchdog identifies misbehaving nodes and pathrater helps routing protocols avoid those nodes. Few existing system deals with selective forwarding attacks which corrupt time critical application, to overcome this factor [12] is proposed where checkpoint based multi hop acknowledgement scheme for detecting selecting forwarding attacks. Acknowledgement based identification are performed through [17][20].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department Of CSE, JayaShriram Group Of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

III . SYSTEM MODEL

3.1 Node Configuration

Deployment phase is considered in node configuration which is further classified into Initialization and Transmission phase.

3.1.1 Initialization Phase

In Initialization phase, sensor nodes are deployed in such as way it is a Directed Acyclic Graph and from that a routing tree is derived. The routing tree keeps on changing and routing behavior is gathered by the sink. Each node is pre loaded with a unique id (sequence number) as well as necessary keying materials which includes secret key, duration to establish pair wise key with other nodes.

3.1.2. Transmission Phase

In transmission phase, packets from the sensor nodes are transmitted through the routing tree. Every node computes two MAC, one using the key shared with the Base Station (BS) and the other using pair wise key that is shared. The node transmits the packet along with the MAC value produced and the forwarding node verifies the data integrity and after verifying the associated MAC value is removed and the corresponding nodes MAC is included and forwarded to the sink. Base Station also verifies data integrity.

3.2 Compromised Nodes Identification Phase

The routing tree is reshaped and compromised nodes are identified using NHCH. In NHCH scheme packet droppers or modifiers are found by clustering the nodes depending on the risk factor and dropping ratio as good, moderate or bad. After finding, the nodes are further ranked to identify most nodes that are sure to drop packets.

3.2.1 Ranking Technique

A routing table is maintained and an accused account is maintained in which nodes are ranked depending on their identification to be bad for several times. The most accused value node is fixed to be bad for sure. The accused value of nodes is reduced by the number of times it has been found together along with the bad node.

3.3 Secure Routing Process

After identifying the compromised nodes a secure route is provided for data transmission. Route is initially discovered and later the founded route is maintained.

3.3.1 Route Discovery and Maintenance

To initiate the Route Discovery, node transmits a "Route Request" as a single local broadcast packet, which is received by (approximately) all nodes currently on the transmission range. Each Route Request identifies the initiator and target of the Route Discovery, and also contains a unique request identification determined by the initiator of the Request? Each Route Request also contains a record listing the address of each intermediate node excluding the compromised that has been identified earlier through which this particular copy of the Route Request has been forwarded.

IV . PERFORMANCE EVALUATIONS

Our proposed scheme is simulated in the ns-2 simulator. For evaluation purpose 30 to 50 sensor nodes are deployed randomly and routing table (source, destination and intermediate node) is created and updated periodically. Initially packets are transferred and nodes that are compromised are identified. The performance is measured with metrics: Residual energy, Detection rate and Delay.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department Of CSE, JayaShriram Group Of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

V . CONCLUSION

In this paper, a simple technique is introduced to identify both packet droppers and modifiers. Packets are transmitted through routing tree along with the MAC values and data integrity is checked by nodes and the sink. The routing is performed to identify the shortest path between each source node and their destination and residual energy is calculated for each node in the network. The routing table is created and updated periodically. The packet will be transmitted through the shortest path. Packet dropping ratio, delay and energy calculations are made to identify the compromised nodes.

REFERENCES

[1] Chuang Wang, Taiming Feng, Jinsook Kim, Guiling Wang and Wensheng Zhang, "Catching Packet Droppers and Modifiers in Wireless Sensor Networks" in IEEE Trans on Parallel Distributed Systems, vol. 36, no. 5, May 2012.

[2] Vijay Bhuse, Ajay Gupta, and Leszek Lilien, "DPDSN: Detection of packet-dropping Attacks for Wireless sensor Networks," Proc. Fourth Trusted Internet Workshop, 2005.

[3] S. Lee and Y. Choi, " A Resilient Packet-Forwarding Nodes in Sensor Networks," Proc. Frouth ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '06), 2006.

[4] R. Mavropodi, P. kotzanikolaou, and C. Douligeris, "Secmr-A Secure Multipath Routing Protocol for Ad Hoc Networks, vol. 5, no. 1, pp. 87-99, 2007

[5]I. Krontiris, T. Ginneetsos, and T. Dimitriou, "LIDeA: A Distributed Lightweigth Intrusion Detection Architecture for Sensor Networks," Proc. Fourth Int'l Conf. Security and Privacy in Comm. Networks (SecureComm '08), 2008.

[6] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. IEEE First Int'l Workshop Sensor Network Protocols and Applications, 2003

[7] F. Ye, H. Luo, S.Lu, and L.Zhang, "Statistical En-Routing Filtering of Injected False Data in Sensor Networks," Proc. IEEE INFOCOM, 2004.

[8] Z. Yu and Y. Guan, " A Dynamic En- route Scheme for Filtering False Data in Wireless Sensor Networks," Proc. IEEE INFOCOM, 2006.

[9] H.Yang, F. Ye, Y.Yuan, S. Lu, and W. Arbaugh, "Toward Resilient Security in Wireless Sensor Networks," Proc. Sixth ACM Int'l Symp. Mobile Ad "Hoc Networking and Computing (MobiHoc '05), 2005S.Zhu, S.Setia, S.Jajodia, and P.Ning, "An Interleaved Hop-by-Hop Authentication Scheme for Filtering False Data in Sensor Networks," Proc. IEEE Symp. Security and Privacy, 2004.

[10] F. Ye, H. Yang, and Z. Liu,"Catching Moles in Sensor Networks," Proc. 27th Int'l Conf. Distributed Computing Systems (ICDCS '07), 2007.

[11] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. ACM MobiCom, 2000.

[12] B. Xiao, B. Yu, and C. Gao, " Chemas: Identify Suspect Nodes in Selective Forwarding Attacks," J. Parallel and Distributed Computing, Vol. 67, no. 11, pp.1218-1230, 2007.

[13] H. Chan and A. Perrig, "Security and privacy in sensor networks," IEEE Computer, Digital Object Identifier vol. 36, no. 10, pp. 103-105, Oct 2003

[14] G.Padmavathi and D. Shanmugapriya "A survey of Attacks, security mechanisms and challenges in wireless Sensor Network," Int'l Journal of Computer science and Information Security (IJCSIS), 2009.

[15] J.M. Mccune, E. Shi, A. Perrig, and M.K. Reiter, "Detection of Denial-of-Message Attacks on Sensor Network Broadcasts," Proc. IEEE Symp. Security and Policy, 2005R. Roman, J. Zhou, and J.Lopez, "Applying Intrusion Detection Systems to Wireless Sensor Networks," Proc. IEEE Third Consumer Comm. Networking Conf. (CCNC), 2006.

[16] B. Yu and B.Xiao, "Detecting Selective Forwarding Attacks in Wireless Sensor Networks," Proc. 20th Int'l Symp. Parallel and Distributed Processsing (IPDPS), 2006.

[17] K. Liu, J. Deng, P.K. Varshney, and K. Balakrishnan, "An Acknowledgement-Based Approach for the Detection of Routing Misbehaviour in Manets," IEEE Trans. Mobile Computing, vol. 6, no. 5, pp. 536-550, May 2007.

[18] X. Zhang, A. Jain, and A. Perrig, "Packet-Dropping Adversary Identification for Date Plane Security," Proc. ACM CONTEXT Conf. (CoNEXT '08), 2008.

[19] B. Barak, S. Goldberg, and D. Xiao, "Protocols and Lower Bounds for Failure Localization in the Internet," Proc. Eurocrypt, 2008.

[20] K. Ioannis, T. Dimitriou, and F.C. Freiling, "Towards Intrusion Detection in Wireless Sensor Networks," Proc. 13th European Wireless Conf., 2007.

[21] A. Srinivasan, J. Teitelbaum, H. Liang, J. Wu, and M. Cardei, "Reputation and Trust-Based Systems for Ad Hoc and Sensor Networks," Proc. Algorithms and Protocols for Wireless Ad Hoc and Sensor Networks, 2008.