INFRINGEMENT PRECLUSION SYSTEM VIA SADEC: STEALTHY ATTACK DETECTION AND COUNTERMEASURE

Prof. Anil Kadam, Ms. Supriya Ghadage, Ms. Naina Verma , Ms. Nikita Sarvade And Swati chouhan

Department of Computer Engineering, Pune University, Pune, India.
supriya0633@yahoo.com
kadam_in@yahoo.com

ABSTRACT

In this paper we are providing a implementation details about simulated solution of stealthy packet drop attack. Stealthy packet drop attack is a suite of four attack types, includes colluding collision, packet misrouting, identity delegation and power control. Stealthy packet drop attacks disrupts the packet from reaching to it's destination through malicious behaviour. These attacks can be easily breakdown the multi-hop wireless ad-hoc networks. Most widely preferred method for detecting attacks in wireless network is behaviour based detection method. In this method a normal network overhears communication from its neighbourhood. Here we are implementing a SADEC protocol which is proposed solution of stealthy packet drop attacks. SADEC overlaid the base line local monitoring. In base line local monitoring each neighbour maintains additional information about routing path also it adds some checking responsibility to all its neighbours. SADEC proves more efficient than baseline local monitoring to mitigate successfully all the stealthy attack types.

KEYWORDS

Misrouting, colluding collision, , identity delegation, wireless ad-hoc network, local monitoring

1. INTRODUCTION

Now a day's wireless networks are becoming more preferable platforms in many domains but security in wireless is very less as compare to wired (traditional) network. They are becoming important platform for command and control of civilian critical infrastructure and military warfare. Stealthy packet drop attack is a latest threat to wireless ad-hoc networks. Here malicious node evades detection and legitimate node treated as malicious node.

It is suite of four attack types which includes:

1. Misrouting: malicious node misroutes the packet to wrong next hop.
2. Colluding collision: Malicious node with help of its colluding partner over flood the valid next hop resulting in packet drop.
3. Transmission power control: malicious node controls the transmission to its nearest neighbor which is not valid next hop and results in packet drop.
4. Identity delegation: Delegate the relay responsibility to its colluding partner which is close to sender.

To detect such attacks such as wormholes and rushing attacks, traditional mechanism like cryptography alone fails. In this paper we are providing a practical implementation details about solution of stealthy packet drop attack is SADEC protocol. Most of researchers use a behaviour based detection mechanism to detect such attacks. Behaviour based detection includes local monitoring (e.g.[7][8]). SADEC also includes local monitoring but adds some checking

responsibility to each neighbour in wireless ad-hoc network along with each guard nodes over the network. SADEC improves the efficiency of the wireless ad-hoc network over the base line local monitoring [1].

Finally, in this paper section 2 contains related work; section 3 contains proposed practical implementation solution to stealthy packet drop attacks. Section 4 contains technology going to be used and features of this project and section 5 contains conclusion.

2. RELATED WORK

Recently, researchers have been exploring many mechanisms to ensure the security of data and traffic in wireless networks. These mechanisms can be divided into the following categories—integrity services and authentication, protocols that use dedicated hardware, protocols that needs clear acknowledgments or use numerical methods. The course variety techniques increase direction strength by first discovering multi way routes [2], [10] and then using these routes to provide redundancy in the data transmission between a source and a destination. The data are preset and divided into multiple shares sent to the target through different paths. Moreover, many of these methods are pricey for resource-constrained networks due to the data redundancy. Also, these protocols could be in hazard to direction sighting attacks, such as the Sybil attack, that prevent the discovery of non adversarial paths.

The authors in [11] commence a technique called packet leashes that uses either fixed time organization or region alertness via GPS hardware. A technique designed to differentiate malicious behaviour regarding cautious dropping of data, relies on open affirmation for recognized data using the equal channel [10], or an out-of-band conduit [12]. This method would cause to be stealthy packet dropping assessable at the end point. The technique incurs high broadcast overhead and have to be superior with other method for scrutiny and separation of the malicious nodes.

Statistical dealings have been used by some researchers for discovery of malicious behaviour, e.g., [13] to detect wormhole attacks. The concern of trust in ad hoc networks has been looked by many researchers (e.g., [14], [15], [16], [17]). All of them use Dempster-Shafer belief theory [18] to incorporate second-hand information which is reported by other nodes to make a standing score of a node. Many approaches which are based on reputation (e.g., [17]) get suffer from deprived protection against ballot stuffing which means a colluding malicious node approving another malicious hop or bad mouthing which means a malicious hop implicating a genuine hop. All the approaches which are based on reputation may get susceptible to performance where a node is functioning correctly but providing incorrect information about a further node or other node. All the approaches can undergo through non convergent behaviour.

For mitigating control and data forwarding misbehaviour in multi hop wireless networks, a broadly used method is cooperative local monitoring [20], [9], [7], [8], [10]. The effort in [10] provides a mechanism to determine paths with definite desirable properties, such as being node put out of joint. Also the efforts in [8] provides discovery of a extensive class of control attacks in opposition to static sensor networks. Though, all the performance-based mechanisms including both communications based and non communication based, as used by researchers to date, not succeed to diminish the stealthy packet drop attack. In [18], introduced the stealthy packet dropping attacks and proposed a protocol called MISPAR to mitigate the attacks.

In this paper, we proposing a practical implementation of isolation of malicious nodes due to both natural errors and framing. Furthermore, this paper provides a proposed implementation details to assess the performance of both BLM and SADEC under-Misrouting and transmission power control attacks.

3. PROPOSED SOLUTION

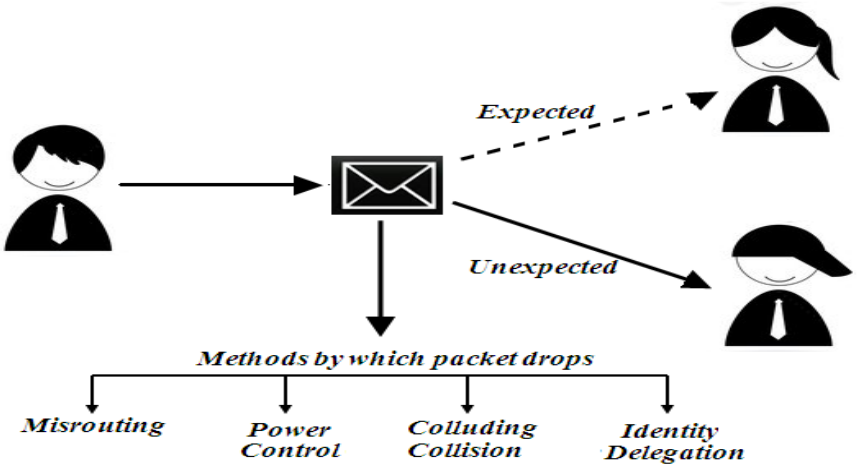

Figure1. Overview of stealthy attack

3.1. Misrouting

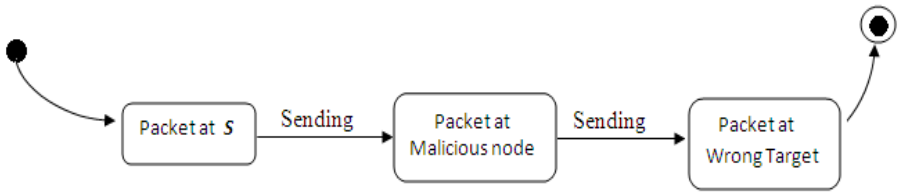

Figure 2(a). Diagram for Misrouting: packet drop attack

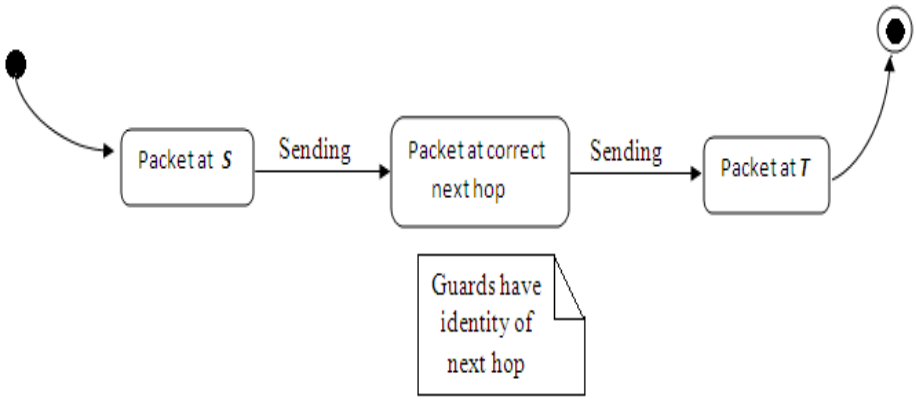

Figure 2(b). Expected Diagram to overcome misrouting packet drop

In figure 2(a) shows that source s sends packet (pkt) to next hop but if next hop is a malicious node then it sends packet to wrong next hop and packet get dropped. To overcome such attack type, in fig. 2(b), source s sends packet to next hop, even though next hop is malicious it can not send packet to wrong hop. Packets get transmitted to valid destination. This can be achieved through SADEC protocol as follows. The guard nodes over the region from source to

destination maintains verification table. Verification table contains the id of all nodes from source node to destination node i.e. it indicates that which node should transmit packet to its next valid hop. Take an example as shown in figure 3 that S is sending a data packet to destination D through a route that includes <A, B, M, X, Y>.

The malicious node M cannot misroute the data packet received from B to another node other than the next hop which is X as each guard of node M over the link B→ M has an entry in its VT (verification table) which indicates X as the correct next hop. This fallout in an additional scrutiny activity for the guard node involved in local monitoring, verifying that the data packet is forwarded to the correct next hop, as indicated by the entry in the guard node's VT. Additionally, M cannot send another neighbour, say Q, by misrouting the packet to Q. The guards of Q over M →Q do not have an entry like <S, D, A, B, M, Q >.

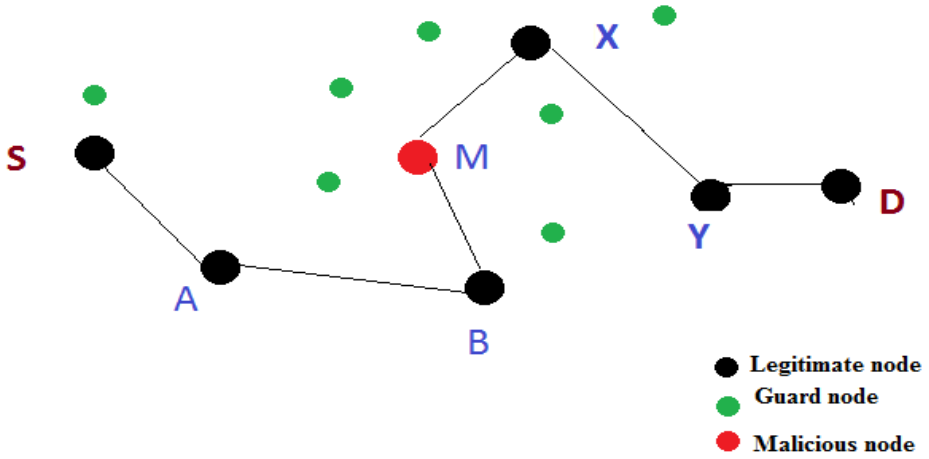

Figure3. SADEC over misrouting

3.2. Colluding Collision

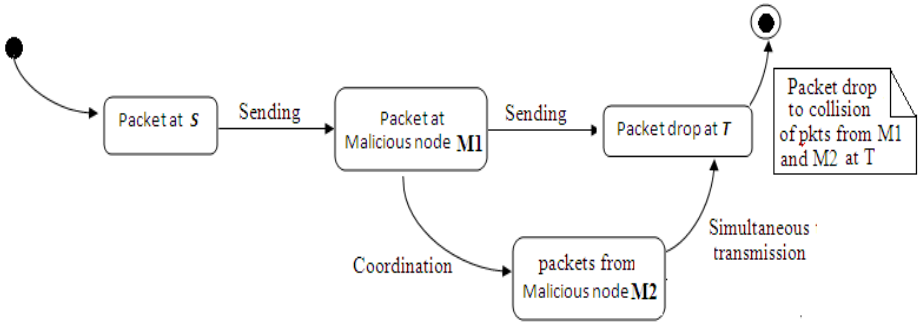

Figure 4.Diagram for Colluding collision: packet drop attack

3.3. Power control

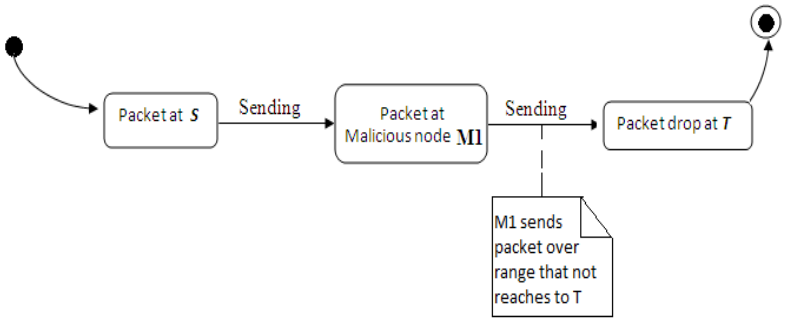

Figure 5. Diagram for power control: packet drop attack

3.4. Identity delegation

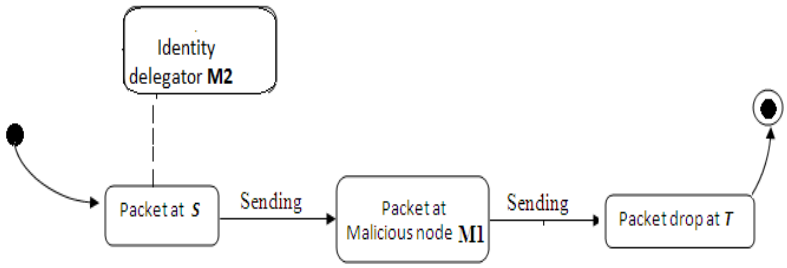

Figure 6. Diagram for identity delegation: packet drop attack

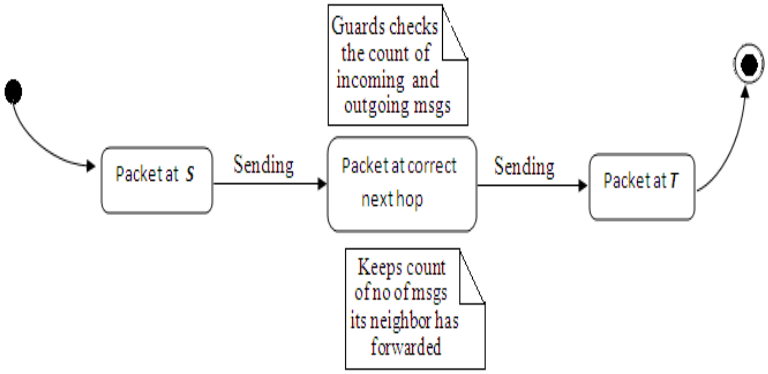

Figure 7.Expected solution to overcome other stealthy attack types

Figure 4 shows colluding collision packet drop attack. In that source node S wants to send packet to target node T. S sends packet to next hop M1. But as M1 is malicious, it coordinates

its transmission activity to its colluding partner M2. The colluding node M2 creates collision at T. as a result node T unable to get packet which is relayed by M1 and packet get damaged. Here, M1 successfully drops the packet and in effect legitimate node T accused of dropping the packet by some of its guard nodes over the transmission region.

Fig 5 shows power control packet drop attack. Here, source node S sends packet to next hop M1 which is malicious. M1 sends the packet to next hop but that not reaches to T i.e. controlled transmission. Similarly in identity delegation packet drop attack as shown in figure 6 , attacker node delegates the identity and credential of compromised node M1 to colluding node M2 which is close to sender node S. when S sends packet to M1, M2 delegates the identity of node M1 and sends the packet. As a result target node T can't hear the message as it not belongs to region of M2. And legitimate node T gets accused of dropping the packet.

Solution to other three stealthy attack type is as shown in figure 7. We have to increase number of guard nodes over the transmission region and adding some extra responsibility to each of the node over network. Each node over the network need to maintain the count of number of messages transmitted by its neighbour and has to announce number of packet it has transmitted over particular period of time. Thus, the subset of guard nodes which had got the packet forwarding would have a greater count than the nodes that did not hear the forwarding of messages. By forcing a node to broadcast the number of messages it has forwarded over certain period of time, a malicious node would have the difficulty of fulfilling two sets of neighbours that look forward to hear different counts through a single broadcast.

4. TECHNOLOGY AND FEATURES

We are going to develop this project in software platform java (jdk1.7.0) with help of JPCAP libraries. The features of this project are as follows:

1. This project provides security in wireless network from stealthy attack.

2. As stealthy attacks are becoming wide spread attack category, prevention of this attack not possible with help of only traditional techniques like cryptography. With help of SADEC [1] protocol efficiency of this project is greater than baseline local monitoring method (BLM).

3. SADEC maintains malicious node detection coverage 90% whereas BLM maintains malicious node detection coverage < 60%. [1].

4. Legitimate node isolation in SADEC is < 2% whereas in BLM it is 99% <. [1].
5. SADEC can deliver 60% packets to valid destination. Whereas, BLM delivers < 10% packets to valid destination

5. CONCLUSIONS

As wireless network threats are becoming more dangerous day by day, security in wireless is most essential. SADEC mitigates all these attacks misrouting, colluding collision, identity delegation, power control successfully with improved efficiency than base line local monitoring scheme. SADEC uses local monitoring scheme and requires nodes to keep up supplementary routing path information and also adds some checking task to each neighbour.

SADEC's new detection approach expands the set of neighbours that are able to monitor in a neighbourhood, thus making it more effective than BLM in sparse networks.

ACKNOWLEDGEMENTS

Our thanks to the experts who have contributed towards development of the stealthy attack and its simulated solution. We would like to thank everyone, just everyone!

REFERENCES

[1] Issa Khalil and Saurabh Bagchi, "Stealthy Attacks in Wireless Ad Hoc Networks: Detection and Countermeasure" IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 10, NO. 8, AUGUST 2011

[2] S.J. Lee and M. Gerla, "Split Multipath Routing with Maximally Disjoint Paths in Ad Hoc Networks," Proc. IEEE Int'l Conf. Comm. (ICC '01), pp. 3201-3205, 2001.

[3] I. Stojmenovic, Handbook of Sensor Networks: Algorithms and Architecture. Wiley, 2005.

[4] F. Ye, H. Luo, J. Cheng, S. Lu, and L. Zhang, "A Two-Tier Data Dissemination Model for Large-Scale Wireless Sensor Network," Proc. Eighth ACM Ann. Conf. Mobile Computing and Networking,pp. 148-159, 2002.

[5] C. Basile, Z. Kalbarczyk, and R.K. Iyer, "Neutralization of Errors and Attacks in Wireless Ad Hoc Networks," Proc. Int'l Conf. Dependable Systems and Networks (DSN '05), pp. 518-527, 2005.

[7] I. Khalil, S. Bagchi, and N. Shroff, "LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks," Proc. Int'l Conf. Dependable Systems and Networks (DSN '05), pp. 612-621, 2005.

[8] I. Khalil, S. Bagchi, C. Nina-Rotaru, and N. Shroff, "UNMASK: Utilizing Neighbor Monitoring for Attack Mitigation in MultihopWireless Sensor Networks," Ad Hoc Networks, vol. 8, no. 2, pp. 148-164, 2010.

[9] I. Khalil, S. Bagchi, and N.B. Shroff, "MOBIWORP: Mitigation ofthe Wormhole Attack in Mobile Multihop Wireless Networks,"Ad Hoc Networks, vol. 6, no. 3, pp. 344-362, May 2008.

[10] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H.Rubens, "ODSBR: An On-Demand Secure Byzantine Resilient Routing Protocol for Wireless Ad Hoc Networks," ACM Trans.Information and System Security, vol. 10, no. 4, 2008.

[11] Y.C. Hu, A. Perrig, and D.B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks," Proc. IEEE INFOCOM, pp. 1976-986, 2003.

[12] B. Carbunar, I. Ioannidis, and C. Nita-Rotaru, "JANUS: Towards Robust and Malicious Resilient Routing in Hybrid Wireless Networks," Proc. ACM Workshop Wireless Security (WiSe '04), pp. 11-20, 2004.

[13] "Statistical Wormhole Detection in Sensor Networks," Lecture Notes in Computer Science, R. Molva, G. Tsudik, and D. Westhoff, eds., pp. 128-141, 2005.

[14] A.A. Pirzada and C. McDonald, "Establishing Trust in Pure Ad-Hoc Networks," Proc. Australasian Conf. Computer Science (ACSC '04), vol. 26, no. 1, pp. 47-54, 2004.v

[15] S. Buchegger and J.-Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes-Fairness in Distributed Ad-Hoc NeTworks," Proc. ACM MobiHoc, pp. 80-91, 2002.

[16] S. Buchegger and J.L. Boudec, "Robust Reputation System for P2P and Mobile Ad-Hoc Networks," Proc. Workshop Economics of Peer-to-Peer Systems, 2004.

[17] S. Ganeriwal, L.K. Balzano, and M.B. Srivastava, "Reputation-Based Framework for High Integrity Sensor Networks," ACM Trans. Sensor Networks, vol. 4, no. 3, pp. 1-37, http://doi.acm.org/10.1145/1362542.1362546, May 2008.

[18] I. Khalil and S. Bagchi, "MISPAR: Mitigating Stealthy Packet Dropping in Locally-Monitored Multi-Hop Wireless Ad Hoc Networks," Proc. ACM Int'l Conf. Security and Privacy in Comm. Networks (SecureComm '08), http://doi.acm.org/10.1145/1460877.1460913, 2008.

[19] G. Shafer, A Mathematical Theory of Evidence. Princeton Univ., 1976.

[20] Y. Huang and W. Lee, "A Cooperative Intrusion Detection System for Ad Hoc Networks," Proc. ACM Workshop Security of Ad Hoc and Sensor Networks (SASN '03), pp. 135-147, 2003

Authors

Prof. Anil Kadam (M.E.Computer Science), AISSMS College Of Engineering, Pune University, Pune, Maharashtra, India.

Ms. Supriya N. Ghadage. (B.E.Computer Science), AISSMS College of Engineering, Pune University, Pune, Maharashtra, India.
supriya0633@yahoo.com

Ms. Naina Verma (B.E. Computer Science), AISSMS College Of Engineering, Pune University, Pune, Maharashtra, India. nainaverma15@yahoo.com

Ms. Swati Chouhan (B.E .Computer Science), AISSMS College of Engineering, Pune University, Pune, Maharashtra, India. chouhanswati@yahoo.com

Ms. Nikita Sarvade (B.E. Computer Science), AISSMS College Of Engineering, Pune University, Pune, Maharashtra, India.