Available online at www.elixirpublishers.com (Elixir International Journal)

Computer Science and Engineering

Elixir Comp. Sci. & Engg. 58A (2013) 14683-14686

ISSN: 2229-712X

Sharon: furtive packet dropping in wireless ad-hoc networks using christina theory

T. Shantha Kumar and D.C Joy Winnie Wise
Department of CSE, Alpha College of Engg, Chennai, T.N, India.

ARTICLE INFO

Article history:
Received: 13 October 2012;
Received in revised form:
17 March 2013;
Accepted: 2 April 2013;

Keywords
SHARON WASN System,
Misrouting, Distance,
Clone node,
Christina Theory.

ABSTRACT
SHARON based Furtive packet dropping is a suite of four afflictions misrouting the distance, clone node, and colluding collision that can be easily established against multi-hop wireless ad hoc networks. Furtive packet falling interrupts the packet from reaching the target through despiteful behavior at an intermediate node. Nevertheless, the entire vindictive node gives the impression to its neighbors that it performs the morganatic forwarding action. Furthermore a legitimate node comes under intuition. We introduce a protocol called FAWAN that can observe and isolate furtive packet dropping affliction efficiently. FAWAN presents two techniques that can be overlaid on baseline local monitoring: having the neighbors maintain additional information about the routing path, and adding some FAWAN provides an innovative mechanism to better a commute local monitoring by considerably increasing the number of nodes in a neighborhood that can do monitoring.

Introduction

WIRELESS Adhoc and Sensor Networks (S-WASN) are becoming an important platform in all several domains, including military warfare and command and control of civilian critical infrastructure. They are especially attractive in scenarios where it is infeasible or expensive to deploy the significant networking infrastructure. Examples in the system field of remote military domain include monitoring of friendly and enemy forces, user equipment and all ammunition monitoring, targeting, and nuclear, biological, and chemical attack detection. Consider a remote military network scenario where more than powerful and less based energy-constrained ad-hoc nodes may be the carried by soldiers or in the vehicles, while a large number of low-cost and low-energy based sensor nodes with limited energy and the resources may be distributed over the battlefield.

This network setup can guide a troop of soldiers to move through the battlefield by detecting and locating enemy tanks and troops. The soldiers can use information collected by the network sensor nodes to strategically position to the nodes for minimize any possible causality. Examples in the civilian domain include habitat monitoring, animal tracking, forest fire detection, disaster relief and rescue, oil industry management, and traffic control and monitoring. However, the open nature, the fast based deployment practices, and the hostile environments where S-WASN may be deployed, make them vulnerable to a wide range of attacks against both control and data traffic Moreover, many S-WASN such as sensor networks are resource constrained, primarily with respect to energy and bandwidth.

An ad hoc network of wireless nodes is temporarily formed network, created, operated and managed by the nodes themselves. It is also often termed an infrastructure-less, self-organized, or spontaneous network. Nodes assist each other by passing data and control packets from one node to another, often beyond the wireless range of the original sender. The execution and survival of an ad-hoc network is solely dependent upon the cooperative and trusting nature of its nodes. However, this naive based dependency on intermediate nodes makes the ad-hoc network by vulnerable to passive and active attacks by malicious nodes.

A number of protocols have been developed to secure ad-hoc networks using cryptographic schemes, but all rely on the presence of an omnipresent, and often omniscient, trust authority. As this paper describes, dependence on a central trust based authority is an impractical requirement for ad-hoc networks. We present a model for trust-based communication in ad-hoc networks that also demonstrates that a central trust authority is a superfluous requirement. The model introduces the notion of belief and provides a dynamic measure of reliability and trustworthiness in an ad hoc network.

Christina Theory & Confidant Nodes

Mobile ad-hoc networking works properly only if the participating nodes have to cooperate in routing and forwarding. However, it may be advantageous for individual nodes not to cooperate.

We propose a protocol, called Christina Theory caters with CONFIDANT, for making misbehavior unattractive; it is based on selective altruism and utilitarianism. It aims at detecting and isolating misbehaving nodes, thus making it unattractive to deny cooperation. Trust relationships and routing decisions are based on experienced, observed based or reported routing and forwarding behavior of other nodes. The detailed implementation of CONFIDANT system in this paper assumes that the network layer is based on the system Dynamic Source Routing (DSR) protocol. We present a performance analysis of DSR It shows that a network with CONFIDANT and up to 83% of misbehaving nodes behaves almost as well as a benign network.

Tele:
E-mail addresses: shancse83@yahoo.com

In multi-hop wireless systems, such as ad-hoc and sensor networks, the need for cooperation among nodes to relay each other's packets exposes them to a wide range of security attacks the system particularly devastating attack is known as the wormhole attack, where a malicious node records control and data traffic at one location and tunnels it to a colluding node, which replays it locally. This can have an adverse effect in route establishment by preventing nodes from discovering routes that are more than two hops away. In this paper, we present a lightweight countermeasure for the wormhole attack, called LITEWORP, which does not require specialized hardware. LITEWORP is particularly suitable for resource-constrained multi-hop wireless networks, such as sensor networks. In this paper, we present a detailed description of the LITEWORP-A for static networks, and discuss extension to mobile networks. Our solution allows detection of the wormhole, followed by isolation of the system malicious nodes. Simulation results show that every user wormhole is detected and isolated within a very short period of time over a large range of scenarios.

Lite Worp Attack- Introduction

In multi-hop wireless systems, such as ad-hoc and sensor networks, the need for cooperation among nodes to relay each other's packets exposes them to a wide range of security attacks.

A particularly devastating attack is known as the wormhole attack, where a malicious node records control and data traffic at one location and tunnels it to a colluding node, which replays it locally. This can have an adverse effect in route establishment by preventing nodes from discovering routes that are more than two hops away. In this paper, we present a lightweight countermeasure for the wormhole attack, called LITEWORP, which does not require any specialized hardware. LITEWORP is particularly suitable for resource-constrained multi-hop wireless networks, such as sensor networks. In this paper, we present a detailed description of LITEWORP for static networks, and discuss extension to mobile networks. Our vital solution allows detection of the wormhole, and it's followed by the isolation of the malicious nodes. Simulation results show that every wormhole is detected and isolated within a very short period of time over a large range of scenarios.

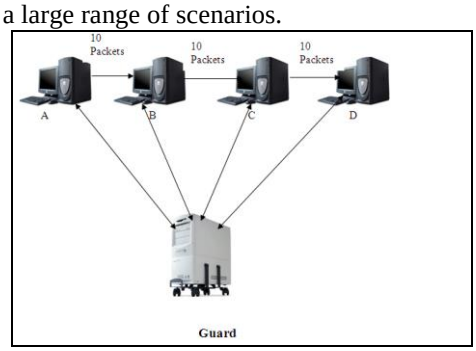

Fig .1. SHARON – WASN guard system model

Fig.1.The guard node is used to find the attack in the nodes based on the input and output transaction of packets, The guard node will be enhance the sharing of resources, operation integration of sectors, and data, and increases throughput in wireless Ad-hoc networks.

FAWAN detection technique involves two high-level steps: first we having basic guard nodes that maintain additional next-hop information gathered during route establishment; and the second, adding some checking responsibility to each neighbor. The latter technique makes use of the fact that under three of the attacks, neighbors have differing views of a node in terms of the amount of nodes forwarding traffic generated by that node. Hence, within a single one-hop broadcast cannot convince all the neighbors.

We expand the set of nodes that can guard a node from only the common neighbors of the node being monitored and its previous hop node to include all the neighbors of the node being monitored.

Mobile ad hoc networking (MANET) has become an exciting and important technology in recent years because of the rapid proliferation of wireless devices. MANETs are highly vulnerable to attacks due to the open medium, dynamically changing nodes network topology, cooperative algorithms, lack of centralized monitoring and management point, and lack of a clear line of defense. In this paper, we report our progress in developing intrusion detection (ID) capabilities for MANET. Building on our prior work on anomaly detection, we investigate how to improve the anomaly detection approach to provide more details on attack types and sources. For several well-known attacks, we can apply a simple rule to identify the attack type when an anomaly is reported. In some cases, these rules can also help identify the attackers. We address the run-time resource constraint problem using a cluster-based with nodes detection scheme where periodically a node is elected as the ID agent for a cluster. Compared with the scheme where each node is its own ID agent, this scheme is much more efficient while maintaining at the same level of effectiveness. We have to conduct extensive based experiments using the NS-2 and Mobile Emulation environments to validate our research.

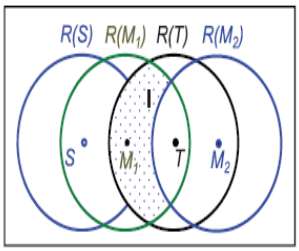

Fig .2. Colluding collision illustration

Fig.2. the malicious node M1 receives a packet from S to be relayed to T and Node M1 coordinates its transmission with a user transmission of some data generated by its colluding partner M2 to T. It has the effect that T is unable to get the packet relayed by M1.

The damage caused by this attack is twofold: 1) M1 successfully drops the packet due to a collision at T without being detected and 2) node T is accused of dropping the packet by some of its guards over the link M 1! T (the guards that are out of the range of M2, region in I). Note that for M2 to be able to send data to T, it has to be a user's legitimate neighbor (compromised by the attack).

Moving circular range queries. In Section 2, we show that it is not possible to extend this technique to the case of the distance-based range queries as the problems of monitoring moving window queries and the distance-based range for queries are inherently different. We apply an aggressive approach to prune the objects/entries that cannot affect the results and/or the safe zone. Our pruning rules are tight and the performance of our solution is close to optimal.

We present an efficient and effective technique to monitor the moving circular range of user queries by adopting the concept of safe zones. We present a rigorous theoretical analysis of mobile tracking to verify the effectiveness of our user safe zone-based approach for the moving circular range queries.

More specifically, we evaluate the probability that a query moves out of the safe zone within one time unit, the expected

distance it travels before it leaves the safe zone, and an upper bound (which is a constant) on the expected number of guard objects for the queries with the diameter of the safe zone no more than a constant times its expected value.

Our experimental results confirm the accuracy of the presented theoretical analysis. We conduct extensive mobile experiments to show the effectiveness of our approach. We compare our algorithm with an optimal solution and a naive solution.

Sharon - Design & Accomplishment

Rushing based Attacks & Defense in Wireless AD

In an ad hoc network, mobile computers (or nodes) cooperate to forward packets for each other, allowing nodes to communicate beyond their direct wireless transmission range. Many proposed routing based protocols for ad-hoc networks will operate in an on-demand fashion, as on-demand with routing protocols have been shown to often have lower overhead and faster reaction time than other types of routing based periodic mechanisms. Significant attention recently has been devoted to the developing secure routing protocols for ad hoc networks, including a number of secure on demand routing protocols that defend against a variety of possible attacks.

In this paper, we present the rushing attack, a new attack that results in denial-of-service when used against all previous on-demand with ad-hoc network routing protocols. For example, DSR, AODV, and secure protocols based on them, such as Adriane, ARAN, and SAODV, are unable to discover routes longer than two hops when subject to this attack. This attack is also particularly damaging because it can be performed by a relatively weak attacker. We analyze why previous protocols fail under this attack. We then develop Rushing Attack Prevention (RAP), a generic defense against the rushing attack for on demand protocols incurs no cost of the unless the underlying protocol fails to find a working route, and provides provable security properties even against the strongest rushing attackers.

SHARON - Furtive Packets Attack Scenario

The Malicious nodes are identified by comparing the number of packets send by the previous Hop with the number of packets received in the period of time. We are extending the work to find out the same process for two Hops also. This process will ensure where the exact malicious behavior is visual exhibited. From this process, we can cloud them easily detect the malicious behavior of the Malicious Node.

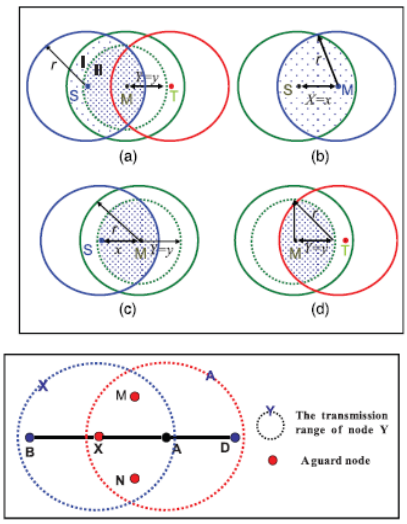

Fig.3. X, M, and N are guards of A over X →A.

Fig. 3, G{X, A}={M, N, X}. Information from each packet sent from X to A is saved in a watch buffer at each guard. The guards expect that A will forward the packet toward the ultimate destination, unless A is itself the destination. Each entry in the watch buffer is time stamped with a time threshold, τ, by which A must forward the packet. Each packet forwarded by A with X as a previous hop is checked for the user corresponding information in the watch buffer. The check can be to verify if the packet is fabricated or duplicated (no corresponding entry in the buffer), then corrupted (no matching hash of the payload), dropped, or delayed (entry is not matched within τ).

Packets Sharing Among Nodes

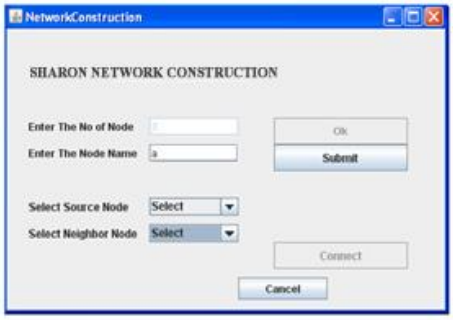

Fig.4. SHARON – NETWORK CONSTRUCTION

Fig.4. The packets will be transferred through the network and share without any miss behavior in intermediate node. In a closed network, nodes are interconnected with and the resources can be shared among them.

For the successful data transfer the network must be properly controlled and handled. This module is designed in order to develop a controlled network traffic environment. All network construction is the module where all the user nodes in the system network interconnected, so as to send the data from one node to the other via network connectivity. As this paper describes, dependence on a central trust authority is an impractical requirement for ad-hoc networks.

We present a model for trust-based communication in ad-hoc networks that also demonstrates that a central trust authority is a system superfluous requirement. The model introduces the notion of the belief and provides a system dynamic measure of reliability and trustworthiness in an ad hoc network.

Conclusion & Future Work

We have introduced a new class of attacks called SHARON furtive packet dropping which disrupts a packet from reaching the destination by malicious behavior at an intermediate node. This can be achieved through misrouting, distance, clone node, malicious jamming at an opportune time, or identity sharing among malicious nodes. However, the malicious behavior cannot be detected by any behavior based scheme presented to date. Specifically, we showed that BLM-based detection cannot be detecting these attacks. Additionally, it will cause a user legitimate node to be accused. We then presented a user protocol called FAWAN successfully mitigates all the presented attacks. FAWAN builds on the local monitoring and requires nodes to maintain additional routing path information and adds some checking responsibility to each neighbor.

We showed through analysis and simulation that BLM fails to mitigate most of the presented attacks while FAWAN successfully mitigates with them. The improvement is seen in terms of increase in the probability of nodes isolation of malicious nodes and decrease in the probability of isolation of legitimate nodes. In future work, we are considering detection techniques for the multichannel multi-radio wireless networks. The user listening activity for detecting malicious behavior is

more complicated due to the presence of multiple channels and multiple radios.

References

[1] A.A.pirzada and C.McDonald,(2007). Establishing Trust in Pure Ad-Hoc Networks , " Proc. Australasian Conf. Computer Science (ACSC '04), vol. 26, no. 1, pp. 47-54, 2004.

[2] Bala Naran.Sastry,U.Shankar,and D.Wagner "Secure Verification of Mobile Location Claims,"Proc.ACM Workshop Wireless Security(WiSe '03),pp.1-10,2003.

[3] S.Ganeriwal, L.Kalmadi Balzano,and M.B.Srivastava, "Reputation-Based Framework for User HighIntegrity SensorNetworks,"ACMTrans.SensorNetworks,vol.4,no.3,pp.1-37,2008.

[4] S.Haiharan,N.Shroff, and S.Bagchi, "Secure Neighbor Discovery in Wireless Sensor Networks,"Technical Report ECE 07-19,Purdue Univ.,2007.

[5] R.Muraleedharan and L.A Osadciw, "Jamming Attack Detection and Countermeasures in Wireless Sensor Networks Using Ant System," Proc.Wireless Sensing and Processing,vol.6248,p.62480G,2006.

[6] D.Ganesan,B.Krishnamurthy, A.Woo, D.Culler, D. Estrin, and S. Wicker, "An Empirical Study of Epidemic Algorithms in Large Scale Multihop Wireless Networks,"Technical Report Intel IRPTR-02-003,Intel Reasearch,Mar.2002.

[7] "StatisticalWormhole Detection in Sensor Networks," Lecturer Notes in Computer Science, R. Molva, G. Tsudik, and D. Westhoff, eds., pp. 128-141, 2005.

[8] 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,"ACMTrans. Information and System Security , vol. 10, no. 4, 2008.

[9] 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.

[10] Y.C. Hu, A. Perrig, and D. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," Proc. ACM Workshop Wireless Security (WiSe '03), pp. 30-40, 2003.

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