Stealthy Attacks in Wireless Ad Hoc Networks

Mahesh Borikar, Swapnil Ghate, Shubham Lande
Computer technology, KDK Collage of engineering
Nagpur, India
borikarmahesh@gmail.com,svapnil.ghate@gmail.com,shubhamlande.sl@gmail.com

***Abstract*: Stealthy packet dropping is a suite of four attacks -misrouting, power control, identity delegation and colluding collision that can be easily launched against multihop wireless ad hoc networks. Stealthy packet dropping disrupts the packet from reaching the destination through malicious behavior at an intermediate node. However, the malicious node gives the impression to its neighbors that it performs the legitimate forwarding action and a legitimate node comes under suspicion. We show that local monitoring, and the wider class of overhearing-based detection, cannot detect stealthy packet dropping attacks. We present a protocol called SADEC that can detect and isolate stealthy packet dropping attack efficiently. SADEC presents two techniques that can be overlaid on basic local monitoring: having the neighbors maintain additional information about the routing path, and adding some checking responsibility to each neighbor .**

***Keywords*: Local monitoring, misrouting, multi-hop wireless networks, packet dropping, transmission power control.**

I. INTRODUCTION

Wireless Ad hoc and Sensor Networks (WASN) are becoming an important platform in 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 significant networking infrastructure. Examples in the military domain include monitoring of friendly and enemy forces, equipment and ammunition monitoring, targeting, and nuclear, biological, and chemical attack detection. Consider a military network scenario where more powerful and less energy constrained ad hoc nodes may be carriedby soldiers or in vehicles, while a large number of low cost and low-energy sensor nodes with limited energy resources may be distributed over the battlefield. This network setup can guide a troop of soldiers to move through the battle field by detecting and locating enemy tanks and troops. The soldiers can use information collected by the sensor nodes to strategically position to 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 deployment practices, and the hostile environments where WASN may be deployed, make them vulnerable to a wide range of security attacks against both control and data traffic. Moreover, many WASN such as sensor networks are resource -constrained, primarily with respect to energy and bandwidth. Thus any security protocol needs to obey these constraints as well Control traffic attacks include wormhole, rushing, and Sybil attacks. The most notable data traffic attacks are blackhole, selective forwarding, and delaying of packets, in which respectively a malicious node drops data (entirely or selectively) passing through it, or delays its forwarding, and misrouting attack in which the attacker relays packets to the wrong next-hop which has the effect that the packet is indirectly dropped. These attacks could result in a significant loss of data or degradation of network functionality, say through disrupting network connectivity by preventing route establishment.

Cryptographic mechanisms alone cannot prevent these attacks since many of them, such as the wormhole and the rushing attacks, can be launched without needing access to cryptographic keys or violating any cryptographic check. To mitigate such attacks, many researchers have used the concept of behavior-based detection which is based on observing patterns in the behavior of neighboring nodes and flagging anomalous patterns. The notion of behavior is related to communication activities such as forwarding packets or non-communication activities such as reporting sensed data. A widely used instantiation of behavior-based detection is Local Monitoring . In local monitoring, nodes oversee part of the traffic going in and out of their neighbors. This leverages the open broadcast nature of wireless communication. Different types of checks are done locally on the observed traffic to make a determination of malicious behavior. For example, a node may check that its neighbor is forwarding a packet to the correct next-hop node, within acceptable delay bounds. For systems where arriving at a common view is important, the detecting node initiates a distributed protocol to disseminate the alarm. We call the existing approaches which follow this template Baseline Local Monitoring (BLM). Many protocols have been built on top of BLM for intrusion detection building trust and reputation among nodes, protecting against control and data traffic attacks and in building secure, routing protocols .For specificity, we will use as the representative BLM which we will use for comparison with the approach presented in this paper. In BLM, a group of nodes, called guard nodes perform local monitoring with the objective of detecting security attacks. The guard nodes are normal nodes in the network and perform their basic functionality in addition to monitoring. Monitoring implies verification that the packets are being faithfully forwarded without modification of the immutable parts of the packet, within acceptable delay bounds and to

the appropriate next hop. If the volume of traffic is high (say for data traffic in a loaded network), a guard node verifies only a fraction of the packets.

In this paper, we introduce a new class of attacks in wireless multi-hop ad hoc networks called stealthy packet dropping. In stealthy packet dropping, the attacker achieves the objective of disrupting the packet from reaching the destination by malicious behavior at an intermediate node. However, the malicious node gives the impression to its neighbors participating in local monitoring that it has performed the required action (e.g., relaying the packet to the correct next-hop en route to the destination). This class of attacks is applicable to packets that are neither acknowledged end-to-end nor hop-by-hop. Due to the resource constraints of bandwidth and energy, much traffic in multi-hop ad hoc wireless networks is unacknowledged or only selectively acknowledged . This is particularly true for the more common data traffic or broadcast control traffic than for rare unicast control traffic.

In this paper, we introduce four modes of the stealthy packet dropping attack. We distinguish between an external malicious node, which does not possess the cryptographic keys in the network, and an internal compromised node, which does and is created by compromising an erstwhile legitimate node. Consider a scenario in which a node called S is forwarding a packet to a compromised node called M. M is supposed to relay the packet to the next-hop node D. The first form of the attack is called packet misrouting. In this mode, M relays the packet to an incorrect next-hop neighbor. The result is that the packet does not reach its intended next-hop while M appears to the guards as doing its forwarding job correctly. The second mode is called the power control attack. In this mode, M controls its transmission power to relay the packet to a distance less than the distance between M and D. Therefore, the packet does not reach the next-hop while the attacker avoids detection by many guards. The third form of the attack is called the colluding collision attack. In this mode, the attacker uses a colluding node (external or internal) in the range of D to transmit data at the same time when M starts relaying the packet to D. Therefore, a collision occurs at D, which prevents the packet from being correctly received by D, while M appears to be performing its functionality correctly. The final mode of stealthy packet dropping is called the identity delegation attack. In this mode, the attacker colludes with a node E placed close to the source node S. E is allowed to use M's identity and transmit the packet. Since E is almost at the same place as S, D does not receive the packet while the guards of M are deceived that M relays the packet to the next-hop. In each of these attack types, the adversary can successfully perform the attack without detection through BLM.

Additionally, in each attack type, a legitimate node is accused of packet dropping. We acknowledge that the attack model calls for smart adversaries e.g., they can collude, can position the adversarial nodes, can control transmission power at a fine level of granularity, or can spend significant energy in launching the attacks. On the other hand, note that these attacks are not hard to mount for motivated attackers since the requirement for successful instantiation of any of these attacks is fairly humble and practically viable . Therefore, we believe that if the network is critical enough, we do have to worry about such motivated adversaries.

II. EXISTING SYSTEM:

Existing work on secure routing attempts to ensure that adversaries cannot cause path discovery to return an invalid network path, but vampires do not disrupt or alter discovered paths, instead using existing valid network paths and protocol compliant messages. Protocols that maximize power efficiency are also inappropriate, since they rely on cooperative node behavior and cannot optimize out malicious action.

Disadvantages of existing system:

- Power outages.
- Due to Environmental disasters, loss in the information.
- Lost productivity.
- Various DOS attacks.
- Secure level is low.
- They do not address attacks that affect long-term availability.

III. PROPOSED SYSTEM:

In proposed system, this setup can guide a connection through the network field by detecting and locating vampire node. The system information collected by sensor nodes to strategically position to minimize any possible causality.

- Protect from the vampire attacks.
- Secure level is high.

In the civilian domain include habitat monitoring, animal tracking, forest fire detection, disaster relief and rescue, oil industry management, and traffic control and monitoring.

Advantages of proposed system:

- Protect from the vampire attacks.
- Secure level is high.
- Boost up the Battery power.
- Ad-hoc networks can have more flexibility.
- It is better in mobility.
- It can be turn up and turn down in a very short time.
- It can be more economical.
- It considered a robust network because of its non-hierarchical distributed control and management mechanisms.
- Group of people with laptops and they want to exchange files and data without having an access point.

IV. MODULE:

1) Local Monitoring:

Cryptographic mechanism alone cannot prevent their attacks since many of them, such as the wormhole and the rushing attacks, can be launched without needing access to cryptographic keys or violating any cryptographic check. To mitigate such attacks, many many researches have used the concept of behavior-based detection which is based on observing patterns in the behavior of neighboring nodes and flagging anomalous patterns. The notion of behavior is related to communication activity such as forwarding packets or non-communication activities such as reporting sensed data .A widely used instantiation of behavior based detection is local monitoring.

2) Multi-Hop Wireless Network:

In multi-hop wireless networks, communication between two end nodes is carried out through a number of intermediate nodes whose function is to relay information from one point to another. Multi-hop or ad hoc, wireless networks use two or more wireless hops to convey information from a source to a destination. There are two distinct applications of multi-hop communication, with common features, but different applications. Two categories:

a) Relay: Tree based topology; one end of the path is the base station. Dedicated carrier owned infrastructure

b) Mesh: Mesh topology, multiple connections among users. Routing by carrier owned infrastructure or subscriber equipment

3) Stealthy dropping attack:

In all the modes of stealthy packet dropping, a malicious intermediate node achieves the same objective as if it were dropping a packet. However, none of the guard nodes using BLM become any wiser due to the action. In addition, a legitimate node is accused of packet dropping. Next, we describe the four attack types for stealthy dropping.

4) Power control stealthy packet dropping.

In stealthy packet dropping, the attacker achieves the objective of disrupting the packet from reaching the destination by malicious behavior at an intermediate node. However, the malicious node gives the impression to its neighbors participating in local monitoring that it has performed the required action. This class of attacks is applicable to packets that are neither acknowledged end to end nor hop by hop. Due to the resource constraints of bandwidth and energy, much traffic in multi hop ad hoc wireless networks is unacknowledged or only selectively acknowledged.

a. Misrouting: A node called S is forwarding a packet to a compromised node called M.M is supposed to relay the packet to the next-hop node D. The first form of the attack is called packet misrouting. In this mode, M relays the packet to an incorrect next-hop neighbor. The result is that the packet does not reach its intended next hop (D) while M appears to the guards as doing its forwarding job correctly.

b. Power Control: The second mode is called the power control attack. In this mode, M controls its transmission power to relay the packet to a distance less than the distance between M and D. Therefore, the packet does not reach the next hop while the attacker avoids detection by many guards.

c. Colluding Collision: In this mode, the attacker uses a colluding node (external or internal) in the range of D to transmit data at the same time when M starts relaying the packet to D. Therefore, a collision occurs at D, which prevents the packet from being correctly received by D, while M appears to be performing its functionality correctly.

d. Identity Delegation: In this mode, the attacker colludes with a node E placed close to the source node S. E is allowed to use M's identity and transmit the packet. Since E is almost at the same place as S, D does not receive the packet while the guards of M are deceived that M relays the packet to the next hop.

V. ATTACKS:

1) Disconnection and Goodput :

An attacker may disconnect a victim in several ways. The first three ways we will describe have in common that the attacker causes a large number of packets to be sent to the victim and its neighbors. This can be done either by ”brute force”, i.e., by simply sending these packets, or by what were for to as the ”stealth DoS”, in which the attacker causes large amounts of traffic to be rerouted by inducing incorrect entries in routing tables of selected nodes.

First, the attacker may route such considerable amounts of traffic through the victim that the victim either runs out of power, since each packet received or sent carries a cost in terms of the battery power consumed. The discussion in on the exact amount of power consumptions support that this is a real threat for standard portable power sources. Second, the attacker may perform a power attack on all known neighbors of the victim node. This will cause disconnection as well, but may be overcome by the victim by him moving into another neighborhood. Third, an attacker may succeed in disconnecting a victim from its neighbors without performing a power attack.

Namely, if the attacker could route large enough quantities of traffic to the victim and its neighbors, causing a portion of these to be dropped (due to insufficient bandwidth), then this could result in a disconnection. This is so since when a router fails in reaching a given node a certain number of times (which is often a parameter of the protocol); the router concludes that the recipient is unreachable.

For both reactive and proactive protocols, the attacker succeeds in disconnecting the victim nodes by making other nodes believe that the former are unreachable (and thus actually making them unreachable). In a fourth type of attack, the attacker does not rely on large quantities of

packets being sent to the victim or its neighbors, but simply uses the weapon for removing an entry (building block _1 or _2) to make the victim node ”disappear”. Receiving a packet from an unreachable node does not yield any routing information unless the packet carries some routing information (e.g., source routing). Moreover, in reactive protocols, if such a disconnected node were to send a packet to one of its neighbors, only that neighbor would know that the victim is reachable. This information will not be advertised to the rest of the network and can therefore be learnt only by neighbor of the victim who is involved in the route discovery process associated with the attack.

Goodput Reduction: We note that disconnecting one or more nodes generally implies a reduction of the goodput of a network. An attacker may mount the attack in several ways. In particular, by disconnecting a large number of nodes, the resulting traffic through the articulation points comes to a crawl; the attacker can corrupt a large enough number of routing tables to increase the de facto traffic through each node (by taking a large number of packets for a ride); and he can degrade the power supplies of a large enough portion of the routers (building block _6) to force them switch to ”egotistic” routing, i.e., only handle their own packets. We note that this may then result in a total disconnection or partition of the network.

2) Reduction Active Eavesdropping:

A second class of attacks aims to “hi-jack” traffic in order to eavesdrop on selected victim nodes. The simplest way to achieve this is to corrupt routing tables of nodes on the path between a victim and the respective sender/receiver. The attacker can remove valid routing table entries and add incorrect ones in order to force rerouting. This can be achieved using the previously introduced building blocks _1, _2, _3, respectively _4. For incoming traffic (i.e., packets going to the victim), the attacker simply forces all traffic to the victim to be sent through a node he has corrupted. In order to select traffic only from certain sources, the attacker may corrupt the routing tables more selectively, allowing those on the path from “not so interesting” sources to remain correct.

For outgoing traffic (i.e., packets sent from the victim to another node in the network), the attacker modifies routing tables of the victim and/or nodes close to the victim (with respect to all “interesting” recipients) thereby causing traffic to be rerouted through a node he controls.

The main difference between proactive and reactive protocols with respect to active eavesdropping are again on how the routing information is tampered and how rerouting is achieved. In proactive protocols, the attacker can simply propagate respective routing tables in which entries are dropped or added. In reactive protocols, the attacker will make use of the route discovery process to advertise new routes or report route error messages. We note that rerouting not only affects traffic from the victim and to the selected receivers, but everybody sending/ receiving packets through any of the routers whose tables are corrupted. The resulting traffic through the eavesdropping node can be reduced by averting all traffic from the corrupted.

VI. PROTOCOLS:

1) Link Layer:

For concreteness, we assume that the link layer protocol follows the IEEE 802.11 standard. Two modes of operation are considered: (i)priority based, contention free Point Coordination Protocol (PCP), and (ii)Distributed Coordination Protocol (DCP) which is based on Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). In CSMA/CA a node listens to the medium until the medium is idle; then it transmits. If there is a collision, the node will hear a different signal in the medium than what it was transmitting, and concludes that the transmission is in collision. Collided stations backup exponentially on the number of unsuccessful attempts to capture the channel. Communication between two stations is based on a 2-way handshake: after authentication, the sender first transmits a Request to Send (RTS) message, and the receiving station replies with a Clear to Send (CTS) message. The sender then transmits data and awaits an Acknowledge (ACK). It is worth noticing that all the management (control) messages are transmitted in the clear in the current specifications of IEEE 802.11. In the following, we limit the focus on security vulnerabilities relating to routing issues, and refer for a discussion of other security concerns relating to this standard.

2) Network Layer:

In the network layer, we assume that one of several available ad-hoc routing algorithms is deployed. We will consider both proactive routing and reactive routing protocols. In the former, nodes maintain a connectivity graph by exchanging routing tables regardless of whether there is demand for routing to every entity in the table. In the latter, routing information is obtained when there is a demand to send traffic to a particular destination. A node updates its routing table only after performing a route request (RREQ) and obtaining a response. In particular, we consider the employment of Dynamic Source Routing (DSR), Ad-Hoc On-Demand Distance Vector Routing (AODV), Zone Routing Protocols (ZRP), and TORA. DSR and AODV are reactive protocols. The former uses route caches while the latter maintains routing tables and uses Distance Vector Routing algorithm to compute the routes. ZRP is a hybrid routing protocol that uses a hierarchical structure for routing. TORA is also a reactive protocol. The attacks considered in this work are relevant to all these protocols.

3) Proactive Routing:

Proactive routing protocols maintain routing tables. When a message is sent using proactive routing, the packet carries only information relating to its origin and desired destination. Each node has a routing table to indicate what the next hop is for that particular destination. Nodes in

proactive routing exchange routing tables periodically – either with neighbors only, or by flooding the entire network. This way, each node can infer the network graph and compute the routes. There are two types of protocols suggested for proactive routing. In link-state protocols and its variants, each node floods its local connectivity (i.e., list of its neighbors and distances to them) to the entire network. Thus, each node knows the (claimed) topology of the entire network and uses Dijkstra's shortest path algorithm to compute the routes. In contrast, distance vector protocols and its variants exchange the global topology information that is maintained only with immediate neighbors. Such algorithms are known to be prone to loops and slow convergence. If the topology of the graph changes during the transmission of a packet (e.g., a link or node goes down), the transient packet will be dropped.

Control messages are propagated periodically, or whenever there is a link failure. Like all network operations, these are asynchronous.

A link failure is recorded locally to the routing table of the node that detects it. The link failure information is propagated to the network by routing table updates using link state or distance vector protocols to prevent routing errors.

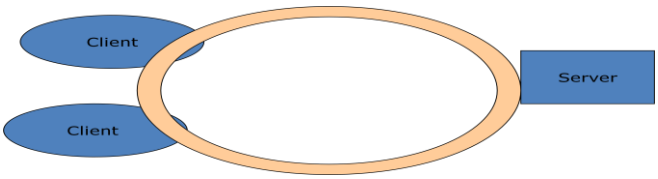
However, an attacker can frequently report link failures to mount additional overflow attacks. Furthermore, such links may not even be real links.

4) Reactive Routing:

While proactive routing protocols maintain routing or connectivity information to a node regardless of whether any packet will ever be sent to that node, in reactive protocols, a route is determined only if there is a packet to be sent. Route discovery information is then stored locally, but may not be communicated to others unless requested. In order to limit the flooding of the network with route requests, and to speed up the route discovery process, some reactive protocols construct and maintain route caches or route tables. (For example, AODV uses local routing tables, while DSR with improvements applies routing caches.) In contrast to routing tables, which only store the next hop (and distance metric) information, a route cache stores the entire route from a source to destination. There is no periodic exchange of route caches: each node "learns" the routing information from the route discovery process. When a message is sent using a source routing protocol (e.g., DSR), the packet carries full routing information, i.e., the sequence of all nodes the packet will traverse. In contrast, in distance vector routing protocols (e.g., AODV), the packets carry only information about their origin and destination. If the graph topology changes during the transmission of a packet, the route will become invalid and transient packets will be lost. Upon receiving a route request message, a node checks its local route information to see if any previously found route for the destination exists. In case of several possibilities, one of them is chosen using a heuristic rule, such as the shortest one, or the shortest one with longest expected lifetime. Large route caches and route tables may contain stale routing information, and so, are often avoided. Due to the size limitation, only the most recent or active routes are maintained. However, small caches or tables can more easily be exploited by an attacker that overflows them with incorrect (i.e., non existing) routes to replace the correct ones to the victim.

VII. WORKING

- Client-server is a computing architecture which separates a client from a server
- It is almost always implemented over a computer network
- The most basic type of client-server architecture employs only two types of nodes: clients and servers.



- Server-create connection for client, manage session, and end connection.
- Client- Request to join server connection and start session, shares data using server connection, end session.

VIII. FUTURE SCOPE:

- Increase security level
- We can use encryption for increasing security.
- This can be a stepping to go further focusing on encryption within connection in network.
- Avoiding intruder from stealthy attack .
- Avoiding packet dropping and decreasing power consumption.

IX. REFERENCES

[1] 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, 2012.

[2] 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, 2012.

[3] 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, 2013.

[4] 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, 2013.

[5] Y.C. Hu, A. Perrig, and D.B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks," Proc. IEEE INFOCOM, pp. 976-986, 2013.