International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) ISSN: 2395-5325
Volume 3, Special Issue 1 (February '2017)
Special Issue on 1st National Conference on Advanced Computing and Communication Technologies,
Conference held at Siri PSG Arts and Science College for Women, Sankari,Tamilnadu,India.

EXPLANATORY DOS ATTACKS IN OLSR PROTOCOL USING DISTRIBUTED FORMATION CONTROL ALGORITHM

S.Sangeetha,
Research Scholar,
Department Of Computer Science,
Theivanai Ammal College for Women,
Villupuram,Tamilnadu,India.

Dr.R.Suguna,
Assistant Professor,
Department Of Computer Science,
Theivanai Ammal College for Women,
Villupuram,Tamilnadu,India.

Abstract : The computerization of critical infrastructure such as control systems means that these systems interact with information technology (IT) to an extent that makes them susceptible to malicious attacks. the main focus of research in routing protocols for Mobile Ad-Hoc Networks (MANET) geared towards routing efficiency, the resulting protocols tend to be vulnerable to various attacks overload. One major DOS attack against the Optimized Link State Routing protocol (OLSR) known as the node isolation attack occurs when topological knowledge of the network is exploited by an attacker who is able to isolate the victim from the rest of the network and subsequently deny communication services to the victim In this paper, we suggest a novel solution to defend the OLSR protocol We develop a model-based resilient control algorithm that enables the team of autonomous agents accomplish their formation task even in the presence of a malicious denial of service (DOS) attack disrupting inter-agent communication.

Keywords: OLSR, node isolation attack, control algorithm, autonomous

I. INTRODUCTION

Today's society increasingly relies on computerized control systems to automate key industrial operations and delivery of critical services. While increased computer interconnectivity over networks has great benefits, a hostile cyber environment poses a security risk to critical infrastructure such as water distribution networks, the power grids and transport infrastructure that is now largely supported by computer systems. Research and recent events have shown that such systems are vulnerable to failure resulting from malicious attacks targeting both physical and communication infrastructure. A number of different routing algorithms exist for network packet transmission. For the most part these algorithms can be classified into two main categories: reactive routing and proactive routing protocols. In the case of proactive (table-driven) protocol, for example, DSDV and OLSR every node constantly maintains a list of all possible destinations in the network and the optimal paths routing to it. Reactive protocols, such as DSR and AODV find a route only on demand. Motivated by the issues mentioned above, strategies that ensure normal operation of networked control systems subject to disturbances and malicious attacks are essential. These are called resilient control Strategies in which the controller is designed to ensure system security. Our objective is to develop a resilient control strategy that ensures normal operation of a multi-agent system in the presence of a DOS attack In this paper we review a specific DOS attack called node isolation attack and propose a new mitigation method. Our solution called We develop a model-based resilient control algorithm that enables the team of autonomous agents accomplish their formation task even in the presence of a malicious denial of service (DOS) attack disrupting inter-agent communication. The OLSR protocol is presented; then, the node isolation attack is described and other previous works related to OLSR MANET security are discussed. A method for protecting OLSR MANET from node isolation attack identify by proposed resilient control strategy. A mathematical model of the system created based on the formation algorithm is implemented alongside the actual system.

2. RELATED WORK

This section briefly presents previous works on data stream clustering, and highlights the most relevant algorithms proposed in the literature in the related techniques is used which is a trust based security techniques in OLSR protocol. The nodes are trust based reasoning to each other node, the identifying the behaviour of malicious node in networks. The mechanisms detect misbehaviour nodes in the networks. The countermeasure and prevention mechanism is used to solve the problems of networks counter and inconsistency of the malicious node in networks. The different attackers and with few modifications, still compatible with OLSR protocol. In the related presented analyze of vulnerability of optimized link state routing protocol against denial-of-service attack. An author proposes the mechanism for OLSR protocol i.e. enhanced OLSR protocol. The techniques are capable to preventing node isolation attack against the OLSR protocol. The technique advertises two extra control packet for finding malicious node from network because of this two control packet adding network traffic increase.

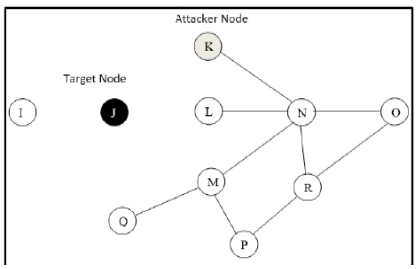

Fig.1 Node O perceives topology after node isolation attack

propose a mechanism to improve the security of the OLSR routing protocol against external attackers. In their solution, each node signs its HELLO and TC messages. These signatures are later used by others to prove their own HELLO and TC messages. The resulting solution prevents devices from declaring imaginary links with known nodes. This solution functions correctly but is expensive in terms of overhead; besides the usual overhead of OLSR, signing messages requires extensive computation, a cumulative factor that grows as the size of the network increases. Another problem is the fact that the network loses its spontaneity as all nodes are required to know each other in advance in order to share their public keys. This prevents the network from evolving naturally from the various nodes that appear at a certain place and time, a fundamental trait of MANETs. Another approach, based on local detection of link spoofing, is given by. The authors provide a number of rules to identify abnormal behaviour on the network. The solution includes a message sent in response to the detection of an intrusion, allowing for the exclusion of compromised nodes and preventing them from being included in network-wide routing tables. Besides the limited scope of the solution, as identification effectiveness is constrained to local nodes only, the ability of sending a warning message is disastrous in itself. Any malicious node can falsely advertise that some other node, local or remote, is malicious, causing for its immediate removal from routing tables all around. In a sense, the solution opens up an attack vector not present in the original problem.

3. SYSTEM ANALYSIS

System analysis is the act, process, or profession of studying an activity typically by mathematical means in order to define its goals or purposes and to discover operations and procedures for accomplishing them most efficiently.

3.1 EXISITNG SYSTEM

Kannhavong et al. attempt to mitigate the problem of colluding attackers. By modifying the HELLO message to include all two-hop neighbours, a node can detect existing contradictions between messages, thus identifying an attack. Raffo et al. propose a mechanism to improve the security of the OLSR routing protocol against external attackers. In their solution, each node signs its HELLO and TC messages. Nadav Schweitzer proposed DOS attack against the Optimized Link State Routing protocol (OLSR) known as the node isolation attack occurs when topological knowledge of the network is exploited by an attacker who is able to isolate the victim from the rest of the network and subsequently deny communication services to the victim. In this paper, we suggest a novel solution to defend the OLSR protocol from node isolation attack by employing the same tactics used by the attack itself. Through extensive experimentation, we demonstrate that 1) the proposed protection prevents more than 95 percent of attacks, and 2) the overhead required drastically decreases as the network size increases until it is non-discernable.

3.2 DISADVANTAGES

1. It is difficult to distinguish between contradictions which occur due to an attack as opposed to those resulting from topology changes.
2. Require either a trusted third party or prior knowledge of network players.

3.3 PROPOSED SYSTEM

In this paper, a team of networked autonomous agents whose collective objective is formation control is used to represent a cyber-physical system. A distributed formation control algorithm in which each agent depends only on its local information and that received from one neighbour to cooperatively carry out the group mission is employed. We develop a model-based resilient control algorithm that enables the team of autonomous agents accomplish their formation task even in the presence of a malicious denial of service (DOS) attack disrupting inter-agent communication. In this paper we review a specific DOS attack called node isolation attack and propose a new mitigation method model-based resilient control algorithm that enables the team of autonomous agents accomplish their formation task even in the presence of a malicious denial of service (DOS) attack disrupting inter-agent communication.

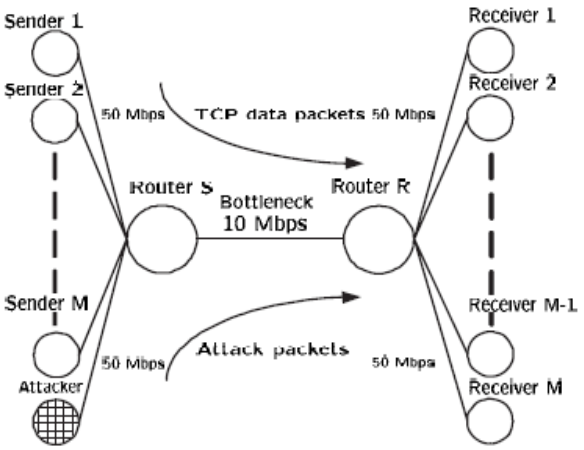

Fig 1. Proposed resilient control strategy

Moreover, DCFM utilizes the same techniques used by the attack in order to prevent it. The overhead of the additional virtual nodes diminishes as network size increases, which is

consistent with general claim that OLSR functions best on large networks. The DoS attack aims at exhausting a victim's system resources, such as memory and CPU, or network bandwidth. In this paper we consider the latter case for which an attacker can employ different ways to flood a victim with spoofed packets. Therefore, the victim sees a sudden surge in the traffic rate coming into its links, causing a high packet dropping rate. We refer this class of attacks to as the flooding-based DoS (FDDoS) attack

3.4 ADVANTAGES

Prevent a node isolation attack in which the attacker manipulates the victim into appointing the attacker as a sole MPR, giving the attacker control over the communication channel.We further strengthened the attack by giving the attacker the ability to follow the victim around.

4. ALGORITHM OR TECHNIQUE

Algorithm 1 Model-based resilient control

Require: Initial state of the actual system $z_s(0)$, Initial state of the Mathematical model $z_m(0) = z_s(0)$

Ensure: Final actual system state z_s^* to accomplish the formation

1: **procedure** MODEL-BASED RESILIENT CONTROL
2: **for** each time step $t \geq 0$ **do**
3: $z_m(t) \leftarrow z_s(t)$ (when no attacks present)
4: $z_s(t) \leftarrow z_m(t)$ ((when an attacks present)
5: repeat for $t = t + \Delta t$
6: **end for**
7: **end procedure**

The proposed resilient control strategy. A mathematical model of the system created based on the formation algorithm is implemented alongside the actual system. It is set to continuously track the true and correct states of agents for resilient control. However, due to the unavoidable difference between the mathematical model and the actual system, the error between the states of the model and the system at any given time can grow significantly large as the states depend on values of the past states. As a result, the model and the system can even reach different steady state values. Our strategy to limit the error between these two sets of states is to use the states of the actual system for calculating the next states of the mathematical model as long as the states of the actual system are not altered or corrupted by attacks. To achieve resilient control, when an attack is detected, the state of the model is used to determine the control action for the agent and the corrupted information coming through the network is ignored. To better illustrate the proposed resilient control strategy, let the actual system.

5. PERFORMANCE EVALUTION

Here we have compared different attack techniques based on its parameters, advantages,disadvantages,technologyandfuturescope.

Algorithms	***Parameters***	***Advantages/Disadvantages***
Active Queue Management (AQM) algorithms	Potential Reach ability Distance	***Adv:*** 1. It identifies the preferable location of the attack 2. Efficient in analyasing the performance reliability ***Dis:*** 1. Lack of continuation 2. Modified identifications are not preferable
Low Energy Aware Cluster Hierarchy (LEACH)	Is one of the most popular hierarchical routing protocols The security of data transfer via wsn is a challenging Issue, especially with the existence of denial of service (dos) Attacks.	***Adv:*** 1. Consumes limited energy 2. Reliable operation 3. Packet delivery ratio, network lifetime and energy consumption are effective ***Dis:*** 1. There may some packet loss 2. Time delay

Active intrusion detection system	Cope up with the congestion, the server reduces the congestion window resulting in throughput reduction	***Adv:*** 1. Validity of detection 2. Capable of injecting packets in to the network in order to create difference between normal and attack scenarios ***Dis:*** 1. Fail to detect the throughput degradation attack. 2. Congestion on the route between the server and client

6. CONCLUSION

In this paper, we proposed a model-based resilient control algorithm that enables a group of agents achieve and maintain formation while under attack. The proposed strategy does not require a highly accurate mathematical model that is often difficult to obtain. In this paper, we suggest a novel solution to defend the OLSR protocol from node isolation attack by employing the same tactics used by the attack itself. We further strengthened the attack by giving the attacker the ability to follow the victim around. We develop a model-based resilient control algorithm that enables the team of autonomous agents accomplish their formation task even in the presence of a malicious denial of service (DOS) attack disrupting inter-agent communication. In our future work, the impact of other attacks such as covert attacks, false data injection attacks, stealth attacks and other deception attacks on multi-agent systems will be considered in order to extend our resilient control algorithm.

REFERENCES

[1] David A. Powner GAO, Critical Infrastructure Protection, Department of Homeland Security Faces Challenges in Fulfilling Cyber-security Responsibilities. Government Report GAO-06 - 1087T, September 2006.

[2] Y. L. Huang, A. A. Cardenas, S. Amin, Z. S. Lin, H. Y. Tsai, and S. Sastry, Understanding the physical and economic consequences of attackson control systems, International Journal of Critical Infrastructure Protection, vol. 2, no. 3, pp. 7383, October 2009.

[3] M. Long, C. H. Wu, and J. Y. Hung,Denial of service attacks on networkbased control systems: impact and mitigation, IEEE Trans. on Industrial Informatics, vol. 1, no. 2, pp. 8596, May 2005.

[4] D. Geer,S ecurity of critical control systems sparks concern, Computer, vol. 39, no. 1, pp. 2023, January 2006.

[5] S. Amin, A. Cardenas, and S. Sastry. Safe and secure networked control systems under denial-of-service attacks. Hybrid Systems: Computation and Control, pp. 31-45, Apr., 2009.

[6] C. Perkins and E. Royer "Ad-hoc on-demand distance vector routing," in Proc. 2nd IEEE Workshop Mobile Comput. Syst. Appl.,Feb. 1999, pp. 90–100.

[7] E. Gerhards-Padilla, N. Aschenbruck, P. Martini, M. Jahnke, and J. Tolle, "Detecting black hole attacks in tactical manets using topology graphs," in Proc. 32nd IEEE Conf. Local Comput. Netw., Oct. 2007, pp. 1043–1052.

[8] C. Adjih, T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, and D. Raffo, "Securing the olsr protocol," in Proc. Med-Hoc-Net, 2003, pp. 25–27.

[9] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks," IEEE Wireless Commun., vol. 14, no. 5, pp. 85–91, Oct. 2007.

[10] D. Dhillon, J. Zhu, J. Richards, and T. Randhawa, "Implementation & evaluation of an ids to safeguard olsr integrity in manets," in Proc. Int. Conf. Wireless Commun. Mobile Comput., 2006, pp. 45–50.