International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.2, 2015

RESEARCH ARTICLE

ISSN: 2321-7758

DEFENDING ON-OFF ATTACK IN WSN BY USING TRUST MANAGEMENT SCHEMES

J.ASHMANTH[1], R.ASWIN SIVA[2], R.KIRUBA[3], M.S.VINMATHI[4]
[1,2,3]Student, [4] Associate Professor, Dept. of CSE, Panimalar Engineering College, India

Article Received: 14/03/2015 | Article Revised on:20/03/2015 | Article Accepted on:25/03/2015

ABSTRACT
A trust management scheme can be used to aid an automated decision-making process for an access control policy. Since unintentional temporary errors are possible, the trust management solution must provide a redemption scheme to allow nodes to recover trust. However, if a malicious node tries to disguise its malicious behaviors as unintentional temporary errors, the malicious node may be given more opportunities to attack the system by disturbing the redemption scheme. Existing trust management schemes that employ redemption schemes fail to discriminate between temporary errors and disguised malicious behaviors in which the attacker cleverly behaves well and badly alternatively. In this paper, we present the vulnerabilities of existing redemption schemes, and describe a new trust management and redemption scheme that can discriminate between temporary errors and disguised malicious behaviors with a flexible design. We show the analytical results of the trust management scheme, and demonstrate the advantages of the proposed scheme with simulation conducted in a Wireless Sensor Network.

1. INTRODUCTION

Trust is an important but complex concept in social science. Trust helps people to make decisions in unpredictable circumstances by reducing the uncertainty. Many distributed systems can be unpredictable and uncertain when the entities try to collaborate with each other. Because of the great number of possible threats in the varying applications that can be deployed through a distributed system, applying trust in such systems can be quite complex. Re-search on trust management schemes, which manage trust and decide policies, has emerged as a challenging issue. Trust management schemes aim to improve collaboration between the entities in a distributed system by predicting future behaviors of peers based on their previous behaviors. Developed by Microsoft, the Windows Presentation Foundation (or WPF) is a computer software graphical subsystem for rendering user interfaces in Windows-based applications. The user interface is an important part of nearly every application. Yet what users expect from those interfaces has advanced significantly. According to our project we are designing our user registration, login and calculating performance through table in our GUI applications. **Business Access Layer (BAL):** BAL contains business logic, validations or calculations related with the

data, if needed. I will call it Business Access Layer in my demo. **Data Access Layer (DAL):** DAL contains methods that helps business layer to connect the data and perform required action, might be returning data or manipulating data (insert, update, delete etc).

2. OVER VIEW OF EXISTING SYSTEM:

Existing trust management schemes that employ redemption schemes fail to discriminate between temporary errors and disguised malicious behaviors in which the attacker cleverly behaves well and badly alternatively. Unfortunately, existing redemption schemes are vulnerable to an On-off attack, which is specifically designed to disrupt the trust management and redemption schemes. By behaving well and badly alternatively, the On-off attack aims to make the trust management scheme consider a bad behavior as a temporary error. Thus, the malicious node would remain active and would have more opportunities to attack the network. Existing redemption schemes do not allow this kind of discrimination of degree of On-off attack.

2.1DRAW BACKS OF EXISTING SYSTEM

There are many trust management schemes that do not employ any redemption at all. Applying Trust In Such Systems Can Be Quite Complex

3. PROPOSEDAPPROACH

A smart attacker may attempt to disturb a trust redemption scheme by behaving well and badly alternatively so that trust is always redeemed just before another attack occurs. This type of attack is referred to as an *On-off attack*. Most trust redemption schemes fail to effectively discriminate between an On-off attack and temporary errors, especially when the majority of the
attacker's behavior is good. Therefore, an attacker may be able to remain active in the system by disguising the attacks as temporary errors. In general, if the malicious node performs *n* good behaviors and *m* bad behaviors alternating, we refer to this as an *nG-mB* On-off attack. Uses a compilation of direct and indirect evaluations to reduce the trust of an On-off attacker to be lower than the trust of other neighboring normal nodes, so the network will detour around the On-off attack nodes in the system.

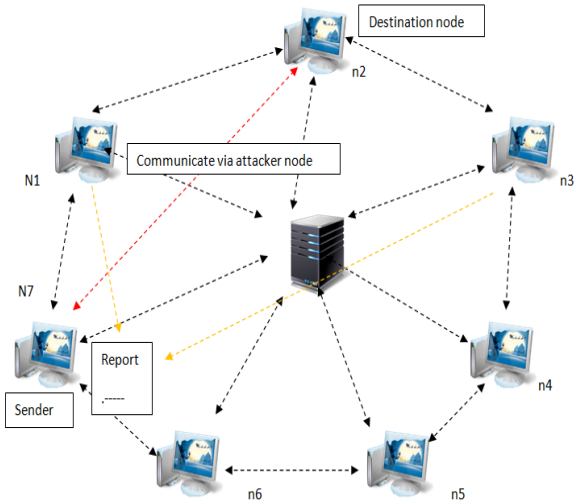
3.1 MERITS:

The On-off attacker did not have an opportunity to continue its attack. We present a new efficient and flexible trust management scheme that detects and defends against On-off attacks.

4.ALGORITHM AND DESIGN

Predictability Trust (PT) is computed based on how well a node's behavior meets expectations. For example, if a node's current forwarding trust is 0.9, we predict that this node will forward at least 90% of the packets that are sent through it. Then in the next round, if this node forwards more than 90% of its packets, it meets the prediction, and is considered to have conducted a Good Predicted Behavior (GPB). If the node forwards fewer than (90 − Δ)% of its packets, it does not meet the expectation, and is considered to have conducted a Bad Predicted Behavior (BPB). Here, Δ is a tunable parameter depending on the application scenarios. In ourexperiments, we set Δ = 0.1. We will count the number of GPBs and BPBs conducted by node *I* (denot-ed by *GPBi* and *BPBi* respectively). The PT of node *i* is com-puted as in (1), using a beta reputation system Bayesian formulation. PT counts the number of the behaviors that did and did not satisfy the designer's expectation. In these simulations, we considered a 100% forwarding transaction as a good behavior

4.1System architecture



5. IMPLEMENTATION DETAILS:

SENDER

Authentication

In authentication module is used to checking the user as valid or invalid. In this module enter the username and password, this username and password is check into the database. If username

and password is correct then allow to next processing, otherwise it consider as invalid user and again go to the login process.

NODE ASSESSMENT

Query forwarding

In this module we describe sender can view the active/inactive nodes. Which is used to classify the active nodes based on their performance and sender can select the active nodes to forward query about such intermediate nodes.

Report view: In this module sender can collect various report from active nodes which will help to asses intermediate nodes through indirect observation. This report contains the information about intermediate node behaviors**.**

Intermediate node selection: In this module indirect observation of sender can analyze report over view then behavior based Selecting high performance node to communicate with receiver node via intermediate nodes**.**

File transfer: In this module sender can assess the node behavior based on indirect observation then choosing intermediate node to file transfer

Block misbehavior nodes: After detection of evil node, we need to drop the communication with that in order to prevent from malware spreading and the evil node details are transferred to database for further reference. Finally evil node gets revoked from the network computer list.

Verify trust recovery; This module used to investigate about trust of nodes by collecting assessments before a normal node get affected by misbehavior. Trust aging process helps to discard outdated assessments of a node and trust consolidation helps to filter negative assessments of a node provided by the other
nodes

Intermediate:

Packet drop & content modification; Packet drop module is used to dropping packets while transmitting file through intermediate node.

Receiver

Files receive & view file details: In this module receiver can receive the file from selected intermediate node and verify the entire detail about received file which is modified or not to assess the behavior of intermediate node.

Update Report: In this module receiver after receiving the file to check the file details and update in database for assessing the intermediate node behavior which will helps to identify misbehavior node and report them to sender node.

CONCULSION

Existing redemption schemes are still vulnerable to the On-off attack. PTR is not only able to avoid faulty detections, but also provides defense against the On-off attack.Proposed system Predictability Trust is a concept that allows for accumulation of previous behaviors to compute trust of a node in a system.

FUTURE ENHANCEMENT

We will focus on evaluating the potential use of the aforementioned test requirements in other testing domains. For example, these requirements may contribute to derive monitoring plans that provide guide-lines about which situations are more interesting to ob-serve at runtime, when the SBA is deployed and executed in the operational environment.

REFERENCES

[1]. I. Akyildiz, W. Su, Y.Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer networks,* vol. 38, no. 4, pp. 393-422, Elsevier, 2002.

[2]. S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," *Proc. of MOBICOM '00*, pp. 255-265, 2000.

[3]. K. Paul and D. Westhoff, "Context aware detection of selfish nodes in dsr based ad-hoc networks," *GLOBECOM'02. IEEE*, vol. 1, pp. 178-182, 2002.

[4]. S. Buchegger and J. Le Boudec, "A robust reputation system for mobile ad-hoc networks," *Proceedings of P2PEcon*, June, 2004.

[5]. P. Michiardi and R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc net-works," *Proceedings of the IFIP TC6/TC11* Sixth Joint Working Con-ference on Communications and Multimedia Security: Advanced Com-munications and Multimedia Security, pp. 107-121, 2002.