A Comprehensive study on threat classification and security service in P2P

M.Seetha, Y.J.Sudha Rani

Abstract—Peer-to-Peer overlay network provide various services for the feature of storing, discovering and locating resources efficiently. P2P platform raise more security-related challenges while providing more services. WhenP2P security mainly focusing on the security problems on Overlay, this paper first shows the how to we classify threat. and how to we provide the security mechanisms to that network. This paper also discuss about the various security services.

KeyTerms: peer peer, threat classification, security services, overlay, underlay

I. INTRODUCTION

Peer-to-Peer (P2P) is a kind of distributed technology characterized by its self-organization ability. P2P network isan overlay network built upon the traditional underlay IPnetwork. Its main function is to store, discover and locate resources efficiently. P2P applications provide various services based on these functions of P2P overlay network.P2P application used to has private protocol and differentnetwork structure. However, with the rapid growth of P2Pservices and the temptation of high scalability and lowmanagement cost P2P provided, people nowadays areworking on open API or open platform of P2P. For example,Skype provides openAPI, many applications have beendeveloped on it. P2PSIP workgroup in IETF is also working on a protocol called RELOAD (REsource LOcation And Discovery)which provides a standard interface to P2Prouting layer. China Mobile even considers providing openP2P platform to build Distributed Service Network, so mobilecustomers can participate in creating and providing servicesjust like on Internet.However, one cost of all the benefits provided by P2Pnetwork is security. There is no doubt that P2P platform willraise more security-related challenges while providing moreservices. Although much has been done on P2P security,but as far as we know, they mainly have been focused on thesecurity problems on Overlay. None has taken underlay intoconsideration.On underlay, each node is a node in traditional network. It has a kind of operation system (OS), network protocol whichin most case now is TCP/IP. As we all know, it faces manysecurity threats, such as virus, cheating, DOS attack, etc. Ifnodes has low security in underlay, attackers may intrude theweak nodes, then penetrate into the whole P2P overlaynetwork through them.iTgives an abstract model of Overlay attackthrough underlay. Through middleware or platform, nodesphysically distributed all across Internet can communicatewith each other to build a distributed network. This networkcan be considered as an overlay network providing someapplications. Alice is in higher security protection withfirewall, while Bob is exposed to attackers without anyprotection, so Bob can be easily attacked. Conventionally, it'sdifficult for attacker to intrude into Alice through underlaybecause of the protection of firewall and intrusion preventionsystems. But in Overlay network, attacker can intrude thedistributed network through node like Bob. Let's assume Bobhas a copy data of Alice on Overlay. Malicious attacker caneasily intrude into Bob to get information of Alice,compromise the confidentiality of the data or even totallycontrol Bob, and attack the whole Overlay network in turn. Cross-layer design can also **coordinate** operations, improving response time and reducing the possibility of security mechanisms in specific layers working at cross-purposes to one another.And also discuss about the peer to peer opeartions in cross alyer design. Frequency hopping in tactical networks mitigates this to some extent, as can power control.Eavesdropping has a low risk due to the low likelihood of gaining access to the application layer.

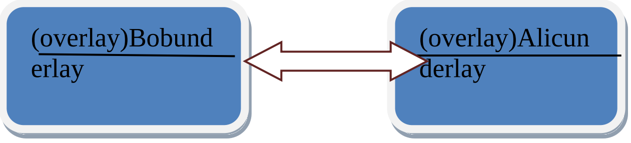

Fig.1 abstract model of Overlay attack through Underlay

So we can conclude that security protection of the nodeson underlay will influence the security degree of distributednetwork. Without proper mechanism, nodes with weakprotection in underlay will greatly deteriorate security of thedistributed network. Unfortunately, with the trend of openAPI and standard protocol, the distributed network mightbecome extremely vulnerable. A new kind of P2P securitymechanism is needed to solve the problem we raise, toimprove the security of whole network effectively.

This paper will show how security threats proliferate inboth underlay and overlay. A security mechanism is thenprovided, in which overlay can be aware of the security postures of underlay, then provides security certificates onP2P network. Node selection or access control can base onsecurity certificate of the node, in order to increase thesecurity of P2P network with lower cost. The paper is organized as follows. summarizesthe related study on security problems of P2P network,illustrates how security threats proliferate between overlay and underlay in open P2P platforms. In this paper also exoalin the how to we classify the threat .

Manuscript published on 30 August 2012.
* Correspondence Author (s)

M.Seetha, Professor,Dept of CSE G.Narayanamma Institute of Technology and Science St.Mary's Engineering College, Deshmukhi, Nalgonda (A.P.), India

Y.J.Sudha Rani. Associate Proffessor Department of CSE St.Mary's Engineering College, Deshmukhi, Nalgonda (A.P.), India

II. THREAT CLASSIFICATION

The key to information protection is maintenance of confidentiality, integrity and availability (CIA). Over time, a number of attacks on networks have been devised each attempting to compromise one or more of the CIA principles. These attacks can be grouped into different types of threats . We consider two main types of threats for tactical networks. Passive threats are based on an attacker who does not emit energy while observing the energy transmitted from other sources. Active threats are based on an attacker who actively transmits energy.

2.1 Passive Threats

Two types of passive threats are considered here. While traffic analysis is of more critical to tactical networks security, both types of network are sensitive to eavesdropping.

2.1.1.Traffic Analysis:

Involves an adversary who collects transmitted energy, traffic flows (protocol headers), sizes, and/or timings to gather insight into the network topology and traffic patterns. This is a serious threat in tactical networks due to their small size, wireless bandwidth and long range. Though message contents cannot be read, the relative importance of nodes and tempo of operation can be determined. Tactical networks are quite vulnerable to this threat as it is straightforward to accomplish with limited knowledge of the network being observed.

2.1.2.Eavesdropping:

nvolves an adversary who examines the content of messages to gather the information transmitted. Again tactical networks are at risk. In this case, the threat is to confidentiality. Tactical networks have a relatively low vulnerability to this threat due to the many layers of security that must be penetrated (up to the application level), but the loss of information privacy could have a significant impact.

2.2 Active Threats

For active threats the adversary transmits at the frequency used by the tactical network. This makes it more dangerous for the adversary as it leaves them open to counter measures (which are not discussed here).

2.2.1.Denial of Service:

Involves an adversary who uses the transmission of packets or raw energy to deny or delay service to authorized participants. There is a wide spectrum of threats, basically one per network layer. At the physical layer, jamming raises the noise floor to the point that nodes in the vicinity cannot decode network traffic . At the network layer the routing protocol might be compromised invalidating packet forwarding or spurious packets can be used to overload the available bandwidth (e.g. gray-hole and rushing). All networks are vulnerable to and impacted by the loss of availability inherent in physical layer attacks. Attacks higher in the protocol stack are made difficult due to the multiple layers of security services.

2.2.2.Masquerade:

Involves an adversary who emulates or acquires one or more valid nodes within a network in order to perform an attack (e.g. wormhole and sybil). This threat is relatively unlikely in tactical networks where the possibility of creating or capturing (and then successfully using) a compatible platform is limited. There is however a significant impact on confidentiality and integrity if such an attack were successful as critical information transmitted could be collected, and potentially modified (see below).

2.2.3.Modification:

Involves an adversary who alters the content (e.g. node exposure and route manipulation) of an intercepted message and then passes it on. The adversary must be an authenticated member of the network in order to accomplish this. A masquerading node is capable of modification up to and including at the application level. Due to the multiple levels of security at each layer, tactical networks are unlikely to be compromised at a high enough level to interfere with the confidentiality and integrity of the network. Compromised availability is the mostly likely result of this type of threat.

III. SECURITYSERVICES

There are advantages to using this peer-to- peer architecture for security in tactical networks. By taking metrics from the security services at one layer, such as from authentication systems and intrusion detection systems (IDS), operations at other layers can be made more secure or optimised. For example, authentication and intrusion detection systems operating at the application layer can provide real-time attack profiles into an integrated security service. The results (metric or metrics) can then be used by the lower layers to improve their efficiency (they don't have to calculate the security metric themselves) and robustness (security is derived from the multiple methods used across the various communication layers). While this framework may increase the complexity and internal processing within a node (in order to integrate multiple functions), it should reduce the communication requirements between nodes (since confirmation with neighbouring nodes is no longer as critical). This is especially beneficial to tactical networks where bandwidth is limited. Some potential security services that could be integrated using this framework are described below.

3.1 Intrusion Detection

Intrusion detection systems (IDS) are employed to determine when the network is being subjected to a network or application layer attack. Such systems are one of the more effective ways to counter, for example, masquerade threats . An IDS can benefit from the establishment of a "trust model", for example, to distinguish among friends, acquaintances and adversaries. An intrusion detection or similar behavioural analysis engine can be charged with monitoring neighbours. In tactical networks, the IDS will likely need to be distributed rather than centralised. This leads to a "watchdog" approach where nodes monitor and analyse the behaviour of their local neighbours. Lessons can be drawn from existing work in the area of Byzantine routing, including consensus algorithms to eliminate falsified information, which can make the system more robust. There are also various methods of establishing trusted routes based on hash chains and digital signatures, but these methods may prove to have too much overhead and consume too much bandwidth to be applicable to tactical networks .

In fact, many of the security overlays proposed in the area of ad hoc networking suffer from overhead issues or complicate the communication protocols such that interoperability among coalition partners could be threatened if different security solutions are employed. Research is being conducted that allows for the provision of security services such as intrusion detection and authentication in mobile ad hoc networks without relying on additional messaging , however it is often the case that detection of an attack at one layer requires mitigation techniques be applied at another. For example, if a Sybil attack), in which a node claims several identities (Masquerade), is detected at the application layer, the response may be to block all traffic coming from the attack's location by eliminating the route from the routingtable .

3.2 Frequency Hopping

Frequency hopping is a well known physical layer defence against frequency jamming. The radio transmits on a set of frequencies in a pre-determined sequence followed by all corresponding nodes in the tactical network. By using frequency hopping, a wider range of the spectrum is used making it more difficult for an adversary to transmit sufficient energy within that band to interrupt the demodulation at the receiver.One of the potential benefits of cross-layer enabling the physical layer is the use of application level characteristics to understand when and to what extent jamming is expected to be a problem. In a time of transmission of critical information, or when the node is in a physical location known to be prone to jamming, the rate and range of frequency hopping can be tuned to the application level requirements based on a security policy. That is, application layer analysis can be used to dynamically modify physical layer attributes.

3.3 Distributed Authentication

For security services in a distributed network, threshold cryptography is generally used to let some or all network nodes share a network master key and collaboratively provide security services such as issuing and refreshing private keys. In a network with N nodes, a group of n special nodes is capable of generating partial certificates using their shares of the certificate signing key. A valid certificate can be obtained by combining k such partial certificates, which is called (k, n)-threshold cryptography. In MANETs, identity (ID)-based cryptography with threshold cryptography is a popular approach for the security design because key management is simpler than that of public key infrastructure (PKI). In threshold schemes, the network can tolerate the compromise of up to (k −1) shareholders. The security of the whole network is breached when a threshold number of shareholders (k) are compromised. Therefore, the optimal selection of nodes in threshold cryptography should be carefully investigated. However, most previous work for key management in this framework concentrates on the protocols and structures. Consequently, how to optimally conduct node selection in ID-based cryptography with threshold secret sharing is largely ignored. In , a distributed scheme based on the stochastic multi-arm bandit formulation is proposed. The proposed scheme can select the best nodes for reconstructing the full secret taking into account the security conditions to minimise the overall threat posed to the network. We can utilize the information obtained from the Metric Store for node selection. For example, we can assign a weight value for a node based on the information from Metric Store. If a node has high security, it may have higher weight. We then conduct the node selection process considering the weights to achieve higher security.

IV. PROBLEM STATEMENT

4.1. Works on P2P Overlay Security

1) Reputationn P2P network, the reputation of a node is a long-termevaluation. Restrict node behavior on the basis of evaluation,or provide the reputation of the node as a reference when choosing a node to cooperate. Usually, node obtains an initialtrust value when joining P2P networks, then it rises or fallsaccording to the node behaviors in the network.

2) Authentication and Access Control

Authentication and access control are the base of Overlaysecurity. Each node owns a unique identity on Overlay.Authentication involves confirming the identity of a node, ensuring what it claims to be is true, while access controldetermines the access permission of the node according touser information. If a node tries to access unauthorizedresources or visit authorized resources without the right way,access control will refuse such attempt and report the incident.

4.2. Traditional Security Solution on Underlay

Compared to P2P overlay, research of traditional security solution on Underlay has a long history. In underlay, partition security domain, provide security protectionon the border ofnetworks, and classified protection are basic solutions. Forexample, firewall in traditional IP network and session border controller in NGN or VOIP network.

CONCLUSION AND FUTURE WORK:

In this paper mainly we are discuss about the Various threat mechanisms and also various security sevices.Mainly these security services apply on the cross layer architecture and also discuss on the P2P network.We are represent the some problems these problems are stasfiy with the help of overlap and underlay security mechanisms.It is only servey about the various threat mechanisms in P2P network.

REFERENCES:

[1] B. Wu,et al. “A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks”, In Wireless/Mobile Network Security. Y. Xiao, X. Shen and D-Z. Du (eds), Springer, 2008.

[2] B. Kannhavong et al. “A survey of routing attacks in mobile ad hoc networks,” in IEEE Wireless Communications Magazine, Vol 14, No. 5, pp 85-91, Oct. 2007.

[3] J.L. Burbank et al, “Key Challenges of Military Tactical Networking and the Elusive Promise of MANET Technology”, IEEE Communications Magazine, Vol 44, No. 11, 2006, pp. 39-45.

[4] S. Jacobs, “Tactical Network Security”, proceedings of IEEE Military Communications Conference, vol. 1, pp. 651-655, Nov. 1999.

[5] Marling Engle & Javed I. Khan，Vulnerabilities of P2P Systems anda Critical Look at their Solutions, Technical Report 2006-11 Internetworking and Media Communications Research Laboratories, Department of Computer Science, Kent State University,http://medianet.kent.edu/technicalreports.html

[6] Ravi Sandhu and Xinwen Zhang. Peer- to-Peer Access Control Architecture Using Trusted Computing Technology. SACMAT’ 05,June 1–3, 2005

[7] B.Crispo, S. Sivasubramanian, P.Mazzoleni, E.Bertino, “P-Hera:Scalable fine-grained access control for P2Pinfrastructures,”Proceedings of the 2005 11th International Conference on Parallel and Distributed Systems (ICPADS'05)