TIME BASED APPROACH FOR SECURITY ENHANCEMENT IN MANET

Mahesh.K.Kaluti*

Paresh Tanna**

Nihil Khagram***

Kapil Patel****

ABSTRACT

Concern to the recent technologies in Mobile Ad-Hoc Networks many scenarios impose a light on establishing secure data authentication, achieving high Throughput, Reliable system design, Strong Cryptographic methods but the recent applications & their vulnerabilities made a new speculated challenges on the security strength of the network, in this paper we demonstrate a mechanism which not only make the system to secure, But it also offers a time based mechanism for data transmission between two nodes & also by enhancing the channel throughput availability by reducing the number of overheads & by eliminating location based errors in the network which is proposed as an extremely flexible technology for establishing High throughput based secure wireless communication in the MANET.

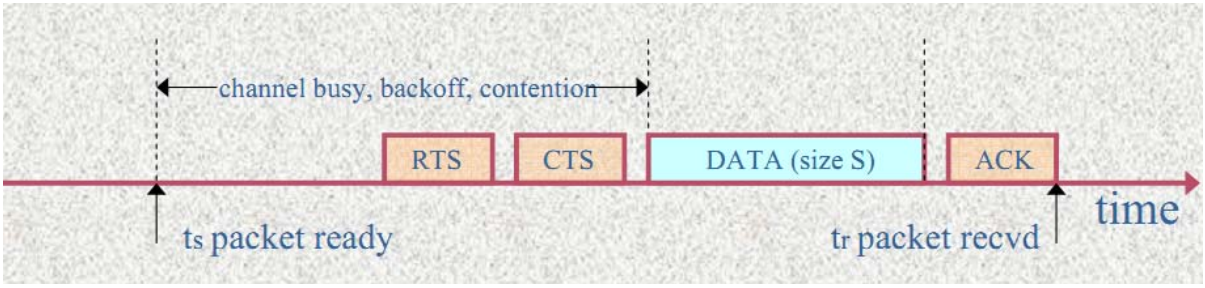
Keywords: *Time-based, Secured, Quality, Robust, Reliable, Flexible.*

*Assistant Professor, Dept of IT, OSEC.

**Assistant Professor, Dept of MCA, RK-University.

***Head, Department of CSE/IT, OSEC.

****Assistant Professor, Dept of IT, OSEC.



In this position paper, we identify the key challenges of building a Peer-to-Peer (P2P) system and outline is that initial steps taken in this direction.

A first question that can be easily posed is why should there by enhancing the channel throughput availability by reducing the number of overheads & by eliminating location based errors in the network which is proposed as an extremely flexible technology for establishing High throughput based secure

P2P solution deferent nodes (used by the users) may use deferent formats to represent the issue tracking overheads and. Data heterogeneity has been a key issue in the system which includes the use of time based mechanism to make the system to secure

The key challenges we identify in building a P2P issue tracking system are:

- Scalability: The inability of the infrastructure to degrade gracefully when the storage, network or processing load grows has impaired such efforts in the past.
- Semantic heterogeneity: Different sources store data in different for- mats or by using different schemas.
- Security: Users must be sure that the data is being shared the way they have specified it. Hence, the need for access control policies and their Enforcement in a purely decentralized or P2P setting is very important

Security issues within Mobile Ad-hoc networks have not yet been widely addressed. A major convict arises from the perceived requirement to provide anonymity for users of networks and an increasing need to provide robust access control, data integrity, confidentiality and accountability services these issues address the cause of the system errors in the existing system. As concern to the security issues the Pseudo-spoofing attacks, in which malicious parties are able to claim multiple identities. For without the foundation of stable, variable identities, it is difficult to provide a set of desired security services. These are increasingly important as industry moves towards using ad-hoc technologies in applications and the security situation for P2P networks is made worse be-cause, by definition, they lack any centralized authority who can vouch for identities or security parameters.

Focusing on security, privacy, and usability, this paperis not about the two main properties that are of typical in-tersest & By Considering incentives, however, leads to new research questions. Traditional bilateral-barter approaches here we are introducing a time based mechanism or the system

SECURE OVERLOADING ISSUES

Eliminate Complex Overlays with Transparency and Automatic Discovery

Application acceleration and WAN optimization solutions that are transparent and integrated into the network fabric do not require network administrators to design complex overlays to control the direction of packet flow for accelerated traffic (on top of existing routed topologies). In addition, such transparent solutions automatically discover one another and maintain crucial pieces of information so that existing services can run uninterrupted and unchanged. Yet most application acceleration and WAN optimization products nevertheless require administrators to deploy overlay networks, fundamentally undermining the investment of time and money spent designing multilayer, resilient, enterprise-class routed networks. Networks today are designed with multiple routes between end nodes, and the network carefully calculates the best path to take based on existing load conditions, distance, bandwidth, and many other metrics. They also apply features to improve the efficiency, security, and control of data at each hop in the path.

An overlays, is a network path-control mechanism that sits on top of an existing routed topology. With an overlay network, static paths must be defined that explicitly control the route that a packet coming from an accelerator must take. When an overlay network is used, rather than allowing the underlying network to determine the path that the flow between two communicating nodes should take, the flow must follow the path that has been explicitly defined between two acceleration devices. It is important to point out that some solutions, while they support auto-discovery when the accelerator is deployed in-line of the traffic flow, they often might not when deployed out-of-path. Thus, the acceleration device undermines the routing decisions that would otherwise have been made by the network. Furthermore, deployment of accelerators that use complex overlay networks makes support for networks with asymmetric or any-to-any routing nearly impossible to provide.

A network-integrated and transparent solution eliminates the need for complex overlay networks, allowing automatic discovery of accelerators. With automatic discovery, shown in Figure 2, accelerators, such as Wide-Area Application Engine (WAE) appliances, first check to see if a peer accelerator exists in the path of packet flow between the source and

destination. If an accelerator exists, an optimization policy is transparently negotiated and then applied to the application flow. If a peer accelerator does not exist, the application flow passes through normally, unchanged.

This provides deployment flexibility in that some locations may require optimization and some may not. Understanding the peering relationships across the WAN ensure that no data is optimized when no peer exists. By using automatic discovery, network infrastructure teams can deploy services to improve application performance over the WAN without having to implement complex overlay networks that require as much, or more, administration than the routed network, maximizing their investment in network and routing protocol design. By using network interception mechanisms such as Web Cache Communication Protocol Version 2 (WCCPv2), physical inline, dedicated load-balancing hardware, or policy-based routing (PBR), along with transparent accelerators that automatically discover one another, IT teams can easily implement application acceleration and WAN optimization within the network.

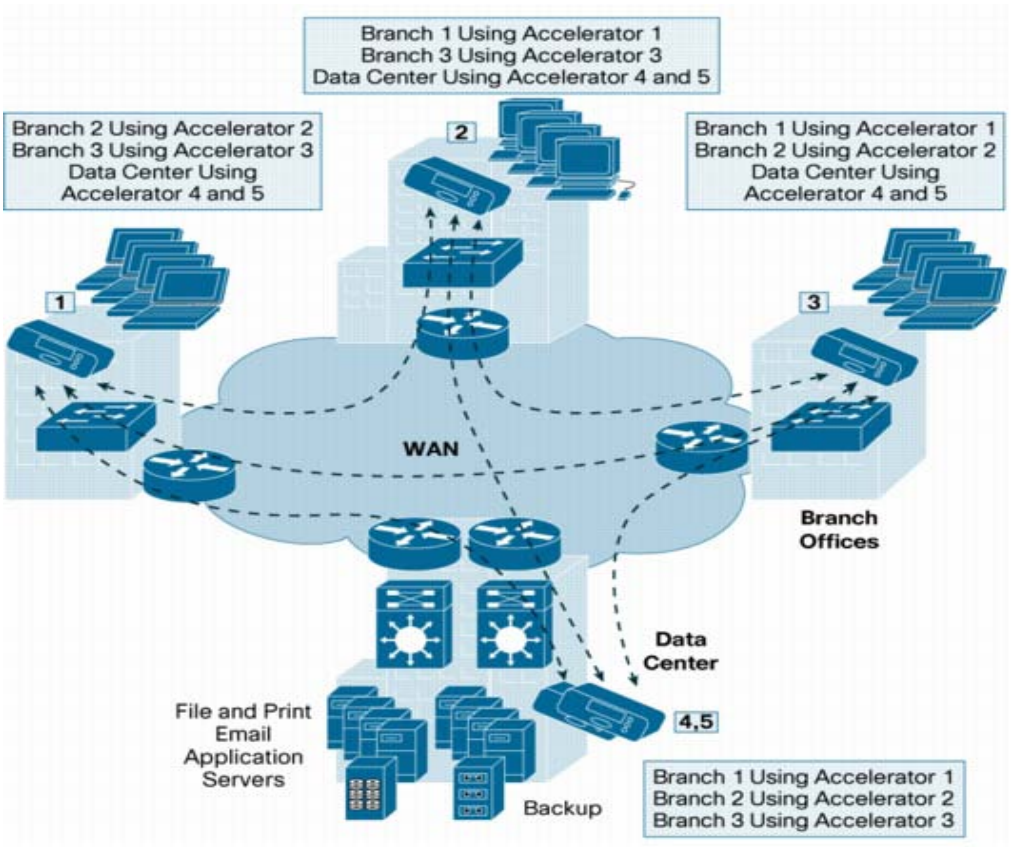


Figure 1. Example of an Overlay

END TO END QUALITY OF SERVICE

Quality fo Service is one example of a service framework that needs to be examined from end-to-end and not just in a couple of places in the network. Deploying QoS in LAN-only

solutions (such as non-integrated, non-transparent accelerators) implements QoS based on only the flows that traverse the device-which is all over the Ethernet network only. In essence, LAN-only QoS have no visibility to WAN conditions or traffic that is sourced in the WAN or by an intermediary network device. Many of the current accelerator products that attempt to provide this QoS functionality are deployed as LAN-side devices and have no visibility to the WAN because they have no physical or logical connection to it. Given that they have no visibility to the WAN and do not act as the network point managing the bandwidth disparity, they can not provide an adequate solution to meet the needs of the demanding enterprise customer. Nor can they provide end-to-end Quality fo Service as they don't act as intermediary nodes at congestion points between communicating nodes.

Network-based QoS delivers much greater flexibility and provides an end-to-end architecture for aligning network resources with application requirements and business priority. The WAN is not merely a "connection"-rather, it is a system in which many applications, some mission-critical, some latency-sensitive, some jitter-sensitive, must all interleave together. Therefore, the network ecosystem from end-to-end must behave as a single entity and common policy and traffic handling characteristics must be ensured.

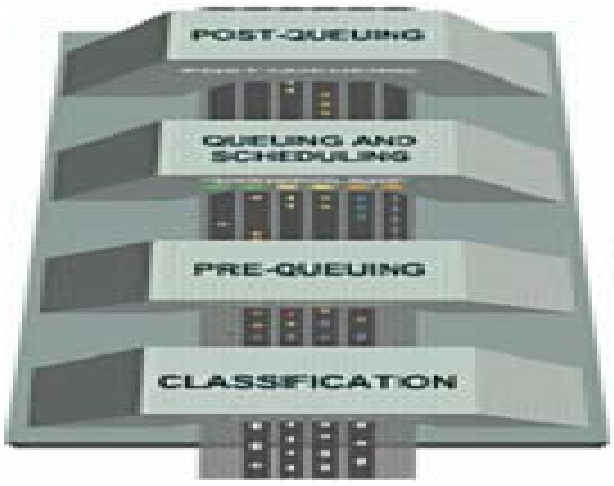


Figure 2. Showing classification of the queuing mechanism

Quality of Service (QoS) is designed to ensure that network resources are aligned with business priority relative to each of the applications being serviced, and configured to handle traffic based on the application requirements. For QoS to be effective, it must be deployed using four key stages:

• **Classification**-the network must be able to identify and classify application traffic based on identifiers that span from the data link layer (layer 2) through the application layer (layer 7) using traditional classification and also deep-packet inspection. This includes data beyond

the typical IP address and port information, and can include source interface, VLAN, application data, packet length, and more. When classification is deployed in the WAN router (or any network device for that matter), with or without the presence of a transparent accelerator, it is then able to adequately identify traffic based on one or more unique identifiers. This identification is then used for the remaining functions of QoS. With non-transparent accelerators, as shown above in figure 4, intermediary network devices such as WAN routers that may be attempting to classify traffic will have no ability to do so. While such non-transparent accelerators may provide some level of classification, they can not provide the same level of classification that is provided within network devices such as WAN routers. Furthermore, as LAN-only devices, they can only classify traffic that they see, which does not include traffic that is generated at the router such as session border control, DLSW, and many other commonly-used protocols [6].

• **Pre-Queuing Operators**-pre-queuing operators are functions applied to traffic before they are queued for service at the point of bandwidth disparity-the WAN. Any time traffic is attempting to traverse a connection, especially those that exist between two links of non-proportionate bandwidth, the traffic must wait in a queue for service. Pre-queuing operators allow the network to apply immediate actions to these flows to improve service and conserve network resources. These operators, such as traffic policing (throttling an application flow to a specified throughput level), packet dropping, counting, bandwidth estimation, and DSCP marking all rely on the ability of the network device itself to adequately identify the application based on one or more classifiers. For transparent accelerators, these features work seamlessly. For non-transparent accelerators, all optimized traffic will be funneled through one or more optimized connections or tunnels, which means that pre-queuing operators such as policing are applied against the tunnel rather than on a per-application basis.

• **Queuing and Scheduling**-not all applications or traffic types are created equal. Some applications require different means of being handled to ensure proper operation or performance. This can be measured in terms of perceived latency, packet loss, jitter, throughput, and other metrics. Queuing and scheduling refers to how packets are handled by devices managing bandwidth disparity and how they are serviced. Cisco IOS has a robust queuing and scheduling architecture that allows for traffic type to be handled based on application requirement and business priority-without compromise. LAN-attached accelerator devices commonly only allow a single type of queuing to be enabled, which can cause significant challenges in converged networks that contain a mixture of voice, video,

and data, where multi-stage queuing and scheduling are necessary. Furthermore, non-transparent accelerators create the additional challenge of rendering network-based classification useless, which means the powerful queuing and scheduling architecture of the network can not be leveraged because traffic flows can not be differentiated.

• **Post-Queuing Optimization**-post-queuing optimization implemented in the network allows for optimized delivery of certain traffic types that require expedited handling under any condition. For instance, link fragmentation and interleaving allows small packets from latency and delay sensitive applications such as Voice over IP (VoIP) to be interleaved between fragments of larger application packets, thus ensuring predictable performance under varying load conditions.

With robust QoS deployed in the network, there is no need to deploy QoS on LAN-attached acceleration devices. By introducing accelerator QoS into the network, I/T organizations run the risk of having to manage two disparate QoS policies to account for scenarios where the accelerator fails and is unable to function, leaving the network itself to manage QoS. This creates the possibility of having overlapping or underlapping policy configurations, not to mention the additional administrative burden of managing QoS in two locations. Cisco WAAS provides the transparency necessary to ensure compliance with existing network QoS configurations.

TIME BASED MECHANISM

The Time Based Mechanism which uses those firms which should have enhanced systematic planning capabilities, & cross functional involvement of itself in the systems related activities, responsiveness to organizational computing demands, high levels of end-user development, and high levels of systems performance. In time based mechanism when a node establishes a route to another node, we will try to check whether there is a link in that route or not by calculating every Round Trip Time (RTT) between two successive nodes along the route. Each node in the established route will compute the RTT between it and the destination, then send this value back to the source node. The source node collects all of these RTT values, calculating RTTs between two successive nodes and identifying required time based on the fact that RTT between any two fake neighbors or two dummy links which will be considerably higher than that between two real neighbors[1].

To calculate the RTT values between two successive nodes we consider the time between an intermediate node sending the RREQ & receiving RREP as Round Trip Time between the intermediate node and the destination. Every node will save the time they forward RREQ &

the time they receive RREP from the destination to calculate the RTT. Given all RTT values between nodes in the route and the destination, RTT between two successive nodes, say A and B, can be calculated as follows:

RTTA, B = RTTA - RTTB

Where RTTA is the RTT between node A and the destination RTTB is the RTT between node B & the destination

For example, the route from S to D includes:

S → A → B → C → D

CONCLUSION

From the above detailed concept it is concluded that recent technologies in Mobile Ad-Hoc Networks many scenarios impose a light on establishing secure data authentication, achieving high Throughput, Reliable system design, Strong Cryptographic methods but the recent applications & their vulnerabilities made a new speculated challenges on the security strength of the network, & also this paper demonstrate a mechanism which not only make the system to secure, But it also offers a time based mechanism for data transmission between two nodes & also by enhancing the channel throughput availability by reducing the number of overheads & by eliminating location based errors in the network.

REFERENCES

[1] R. Poovendran and L. Lazos. A graph theoretic framework for preventing the wormhole attack in Wireless Ad Hoc Networks, to appear in ACM Wireless Networks.

[2] Issa Khalil, Saurabh Bagchi, Ness B. Shroff, LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks, International Conference on Dependable Systems and Networks (DSN 2005): 612-621

[3] Hon Sun Chiu King-Shan Lui, DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks, International Symposium on Wireless Pervasive Computing ISWPC 2006.

[4] Phuong Van Tran, Le Xuan Hung, Young-Koo Lee, Heejo Lee, Sungyoung Lee, TTM: An Efficient Mechanism to Detect Wormhole Attacks in Wireless Ad-hoc Networks, Wireless Sensor Network Track at IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, USA, Jan 11-13, 2007.

[5] D. Boneh and M. K. Franklin. Identity-based encryption from the weil pairing. In Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, pages 213–229. Springer-Verlag, 2001.

[6] R. Canetti, O. Goldreich, and S. Halevi. The random oracle methodology, revisited (preliminary version). In STOC, pages 209–218, 1998.

[7] M. Castro, P. Druschel, A. Ganesh, A. Rowstron, and D. Wallach. Secure routing for structured peer-to-peer overlay networks. In Proceedings of OSDI 2002, Boston, MA, Dec. 2002.

[8] L. Chen, K. Harrison, N. Smart, and D. Soldera. Applications of multiple trust authorities in pairing based cryptosystems. In Proccedings of the Infrastructure Security Conference 2002, volume LNCS 2437, pages 260–275, 2002.

[9] Camp L.J. (2003) Design for Trust. In R Falcone (Ed.) Trust, Reputation and Security: Theories and Practice (pp. 15-29) Berlin:
Springer-Verlang.

[10]Castro M., Druschel P., Ganesh A., Rowstron A., & Wallach D.S., (2002) Security for Peer-to-Peer Routing Overlays. Fifth
Symposium on Operating Systems Design and Implementation (OSDI '02), Boston, MA.

[11]A. Anagnostopoulos, M. T. Goodrich, and R. Tamassia. Persistent authenticated dictionaries and their applications. In Proc. ISC, pages 379–393, 2001.

[12] J. Aspnes and G. Shah. Skip graphs. In Proc. ACM-SIAM Symposium on Discrete Algorithms, pages 384–393, 2003.

[13] M. Castro, P. Druschel, A. J. Ganesh, A. Rowstron, and D. S. Wallach. Secure Routing for structured p2p overlay networks. In Proc. OSDI, pages 299–314, 2002.

[14] F. Dabek, M. F. Kaashoek, D. Karger, R. Morris, and I. Stoica. Wide-area coop-erative storage with CFS. In Proc. SOSP, pages 202–215, 2001.

[15] P. Devanbu, M. Gertz, A. Kwong, C. Martel, G. Nuckolls, and S. Stubblebine. Flexible authentication of XML documents. In Proc. CCS, pages 136–145, 2001.

[16] P. Devanbu, M. Gertz, C. Martel, and S. G. Stubblebine. Authentic data publication over the Internet. Journal of Computer Security, 11(3):291–314, 2003.

ACKNOWLEDGEMENT

Authors are thankful to the Department of Information Technology of Omshanti Engineering college, and Department of MCA of R.K.School of Engineering, for providing infrastructure facilities during progress of the work. Also a lot of people helped us like our students and their support to make completion of this work successfully. Authors are grateful to everyone who contributed with data to make this project successful.