Investigating Anonymous and Secure Fault-Tolerable Routing Protocols for Overlay Networks

Chia-Chen Wu
National Chiao Tung University
chiachen.cs95g@gmail.com

Yu-Lun Huang
National Chiao Tung University
ylhuang@cn.nctu.edu.tw

Shiuhpyng Shieh
National Chiao Tung University
ssp@cs.nctu.edu.tw

Abstract - Anonymity is important for both data requests and responses in IoT applications running on overlay networks. Overlay routing reveals information since identities are required to locate and obtain sensor data from nodes (i.e. IoT devices). An anonymous and secure fault-tolerable routing protocol is hence required to provide anonymity against adversaries and tolerance of node failures. In this paper, we discuss and compare the existing anonymous systems in terms of key management, storage cost and anonymity. To secure a communication session, confidentiality and integrity should be provided. Layered encryption algorithms are then recommended to secure messages flowing through an overlay network. To provide anonymity, it is ideal to have every node along the path only know its previous and next hops, so that an intermediate node can identify neither the initiator nor the responder. To guarantee fault tolerance, grouping nodes within a certain distance or with the same prefix is recommended. Thus, any node on the routing path can easily take over message forwarding if any of its group nodes is detected inactive or failed.

Keywords - IoT security, overlay networks, anonymity route, fault-tolerance

I. INTRODUCTION

Security, productivity, connectivity and management bring the growth of IoT services running on overlay networks. Overlay networks [1] can decouple network addresses from physical placements of peers and enable Internet-of-Things (IoT) applications (see Figure 1). IoT applications allow users to request information and control devices (such as home appliance) remotely. Anonymity and security hence become much more important when IoT users and devices are communicating with each other [2]. Without protection, an adversary lurking in an IoT network may easily trace the communication peers and eavesdrop the conversation between nodes. A protocol securing the routing paths and providing anonymity is hence required for anonymity protection in such cases.

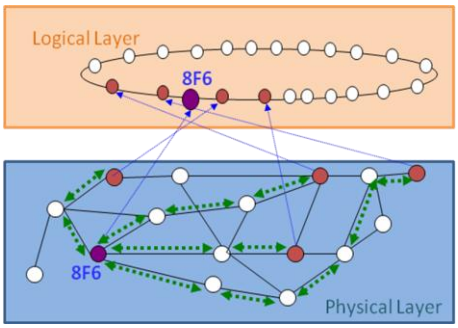


Figure 1 Overly Networks

In the past few years, researchers investigated different kinds of anonymity methods, including initiator anonymity, responder anonymity and relationship anonymity (unlinkability), for overlay and peer-to-peer networks [3][4][5][6][7]. Initiator anonymity hides the identity of an initiator to all other peers in the network, while responder anonymity hides the responder from all other peers. If both initiator anonymity and responder anonymity are provided, mutual anonymity is then guaranteed. Relationship anonymity ensures the unlinkability between an initiator and its responders. Nodes helping forward messages cannot locate the source and destination of a conversation.

Most anonymity related systems, such as Onion Routing [8], make all anonymous connections go through a fixed set of trusted nodes (e.g. IoT gateways), which are not preferred in decentralized overlay networks. By monitoring the traffic of either a colluding entry or exit, adversaries may easily identify the initiator or responders during any communication session. Failure of any fixed nodes along a routing path results in data

loss and larger jitter before the routing path is recovered or a new path is constructed.

Since 2000, many methods, including Surepath[3], Onion Routing [8], Crowds [9], Tarzan [10], , Tor [11], Cashmere[12], Agyaat [13], and Aqua [14] have been designed to exploit peer-to-peer overlays in anonymous communication. A number of random nodes are used to build up anonymous paths or tunnels. In these methods, messages delivery will be failed if any node along the route fails or misbehaves. When there is an error in the route, it is generally difficult for an initiator to locate the failure node. Consequently, the initiator needs to reconstruct another routing path for delivering messages. Frequent reconstruction of routing path, however, exposes the initiator to eavesdroppers and attacks. Hence, a secure, anonymous and fault-tolerable routing protocol is required for enhancing the route reliability for overlay services and IoT applications.

In this paper, we discuss the existing anonymous systems for overlay networks and explain the possibility to adopt layered encryption and random intermediaries to achieve anonymity and guarantee unlinkability between an initiator and its responders.

II. ANONYMOUS SYSTEMS

The section briefly introduces some of the popular anonymous systems, such as Crowds, Onion Routing, Tarzan, Tor, Cashmere, Agyaat, and Surepath.

In Crowds [9], no encryption is adopted. Any node on the path can observe the conversation traffic. Crowds can provide some anonymity by routing messages through anonymous paths involving a randomly chosen sequence of nodes. The initiator sends the message to a randomly-chosen node called "jondo." Upon reception, each jondo randomly decides to either send the message to the responder or forward it to another jondo. In Crowds, anonymous paths are vulnerable to node failures. Node failures pose a functionality problem for anonymous paths.

Onion Routing[8] uses a static set of dedicated onion routers to redirect network traffic. Before sending a message, the sender selects a set of currently active routers to forward through. Session keys are distributed to the chosen routers during the setup phase. The initiator creates an onion by encrypting the message with the public key for every router in the routing path. To transfer a message, each router decrypts the outside layer with its private key. After that, the router discovers the next hop and forwards the message. Every relay node knows only its previous and next hops. Node churns, frequent node arrivals, departures, and failures, limit the scalability of Onion Routing.

Tarzan [10] provides anonymity with high resistance against traffic analysis by using layered encryption, multi-hop routing, cover traffic and a special mix selection protocol. The source chooses a set of relays to act as a path and iteratively establishes a tunnel through these relays with symmetric keys between them. The creation of a tunnel incurs both significant computation overhead and delay. The source wraps the packets in several layers of encryption and sends it through relay nodes. The relay node strips off one layer and sends it to next relay node, etc. Since none of the peers on a tunnel knows the whole path, an adversary cannot figure out communicating peers. Tarzan is still vulnerable if an adversary can observe traffic throughout the Internet. Another vulnerability of Tarzan is the resilience of node failures. Node failures pose a functionality problem for anonymous paths. Also, responder anonymity is not guaranteed in Tarzan.

Tor [11], the second generation of Onion Routing, is one of the most popular privacy enhancing systems. Tor provides mutual anonymity against non-global adversaries using rendezvous points. Tor uses a directory server to maintain router information, which limits the scalability. If the first or last router is compromised in an Onion Routing network, either source or destination can be revealed. Recent work also shows that the Tor anonymity network is vulnerable to the attack in which eavesdroppers may exploit the homogeneous routing policy by falsely advertising high bandwidth links, drawing traffic towards the nodes under its control.

Cashmere[12], a resilient anonymous routing system on structured overlay networks, provides both source anonymity and unlinkabality of source and destination. Cashmere is designed to use a prefix-routing based on structured overlay network, such as Tapestry and Pastry. As shown in Figure 2, nodes with the same prefix form a group. The routing path used in Cashmere is a set of distributed relay groups rather than a single node. Layered encryption is then applied on the routing path by the public/private key pair shared with all members of each relay group. Except all the members of the relay group in the routing path fail, the routing path is remained valid. The source node can randomly reorder the relay groups to hide the destination relay group containing the destination node.

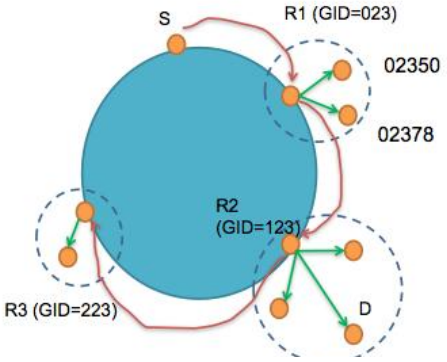


Figure 2 Cashmere

Agyaat [13] provides a compromise between anonymity and efficiency by means of a two-level hybrid architecture. In this system, the initiator can flood its request to every peer in its cloud. At the responder's end, some peers in the cloud of the responder get the request and then broadcast it in its cloud. Agyaat makes a key map onto a cloud linking to an appropriate peer.

In SurePath[3], a node seeking initiator anonymity generates a small number of RSA session keys, deploys the RSAs into an overlay network using distributed hash table (DHT), forms an anonymous path using a subset of the deployed RSAs, and sends messages through the resulting anonymous path, as illustrated in Figure 3. Leveraging the DHT routing infrastructure and data replication mechanism, SurePath is fault-tolerant to node failures. Nodes with similar identities can form a group and nodes in the same group can help forward messages if any node in the group fails. However, a malicious node can disclose the RSAs stored in its local storage to other colluding nodes such that the malicious nodes can pool their RSAs to break anonymity of other users.

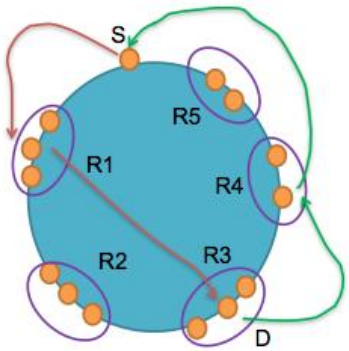


Figure 3 SurePath

More, no mechanism is provided in SurePath for detecting compromised tunnels. SurePath users need to reform their tunnels periodically to resist against the colluding malicious nodes.

III. COMPARISON

To secure communication sessions, confidentiality and integrity should be provided. Layered encryption algorithms are then recommended to secure messages flowing through an overlay network. To provide anonymity, it is ideal to have every node along the path only know its previous and next hops. Hence, an intermediate node can identify neither the initiator nor the responder. To guarantee fault tolerance, grouping nodes within a certain distance or with the same prefix is recommended. Thus, any node on the routing path can easily take over message forwarding if any of its group nodes is detected inactive. This section compares the existing anonymous systems in terms of key distribution, storage cost and anonymity.

(1) Key distribution and discovery

Since node identity is used as node's public key, newly joined nodes in Cashmere do not affect the existing nodes. In SurePath, adding or deleting a node requires extra key distribution or index management. The performance of SurePath decreases as the number of nodes in overlay networks increases. More, Tarzan, Onion Routing, SurePath, Cashmere use layered encryption and multi-hop routing to achieve anonymity. Hence, a trusted third party (like Certificate Authority) is required to generate public keys for protecting data secrecy. However, if algorithms like Fuzzy identity-based encryption scheme [15] is used, key generation and encryption can be done without CA involvement.

(2) Storage cost

Storage cost is one of the concerns when deploying security mechanism to IoT networks. In Cashmere, every node having an *m*-bit identity needs to keep *m* public keys and *m* private keys corresponding with each identifier prefix. In SurePath, each node stores several keys, including its private key, public keys of other nodes and the corresponding symmetric keys for relay sets.

(3) Anonymity

The systems and methods mentioned in the previous section are designed for generating anonymous routing path that provides initiator anonymity. Among them, SurePath forwards and replies messages via different routing paths so that they can prevent the traffic being analyzed by an adversary. For responder anonymity, SurePath and Cashmere know not only the data name but also the public key of the node storing the data. Considering a network in which every node has an *m*-bit identity, and an attacker has compromised a node in the network, 1) if the network runs with Cashmere, the attacker can obtain *m* public keys and *m* private keys associated with the prefix of the compromised node; 2) if the network runs with SurePath, the attacker can control *N-1* share keys where *N* is the network size.

IV. CONCLUSION

To secure communications for peer-to-peer or IoT applications (like smart home appliance control) running on an overlay network, a secure, anonymous and fault-tolerant routing protocol should be designed to provide anonymity against adversaries. Layered encryption and random intermediaries can be adopted to achieve anonymity for overlay networks. By grouping nodes with the same prefix or within a certain distance, and applying algorithms like Fuzzy identity-based encryption scheme, a node is allowed to decrypt the ciphertext encrypted with any other's public key if and only if the two nodes belong to the same group or are within a certain distance. Thus, any node can easily take over message forwarding if its neighboring node fails. Unlinkability between

initiator and responder should also be guaranteed by unlinking an immediate node and its previous node and next node. In the paper, we compare the existing anonymous systems in terms of key management, storage cost and anonymity to show how the existing systems work for routing messages in an overlay network.

REFERENCES

[1] Eng Keong Lua, Jon Crowcroft, Marcelo Pias, Ravi Sharma and Steven Lim, **"A Survey and Comparison of Peer-to-Peer Overlay Network Schemes,"** IEEE Communications survey and tutorial, Mar. 2004.

[2] Nguyen Phong Hoang and Davar Pishva, **"A TOR-based Anonymous Communication Approach to Secure Smart Home Appliances, "** in Proc. of 17th International Conference on Advanced Communication Technology (ICACT), PP. 517 – 525, 2015.

[3] Yingwu Zhu and Yiming Hu, **"SurePath: An Approach to Resilient Anonymous Routing,"** International Journal of Network Security (IJNS) Mar. 2008.

[4] Nikita Borisov, and Jason Waddle, **"Anonymity in Structured Peer-to-Peer Overlay Networks,"** Technical report, UC Berkeley, May 2005.

[5] Michael Kinateder, Ralf Terdic, and Kurt Rothermel, **"Strong pseudonymous communication for peer-to-peer reputation systems,"** ACM Symposium on Applied computing, Mar. 2005.

[6] Paul Syverson, Gene Tsudik, Michael Reed, and Carl Landwehr, **"Towards an Analysis of Onion Routing Security,"** In Proc. of PET, July 2001.

[7] K. Bauer, D. McCoy, D. Grunwald, T. Kohno, and D. Sicker, **"Low-resource Routing Attacks Against Anonymous Systems,"** Technical Report CU-CS-1025-07, University of Colorado at Boulder, Feb 2007.

[8] Paul F. Syverson, David M. Goldschlag, and Michael G. Reed, **"Anonymous Connections and Onion Routing,"** IEEE Journal on Selected Areas in Communication, Special Issue, 1998.

[9] Michael K. Reiter and Aviel D. Rubin, **"Crowds: anonymity for Web transactions,"** ACM Transactions on Information and System Security, 1998.

[10] Michael J. Freedman and Robert Morris, **"Tarzan: a peer-to-peer anonymizing network layer,"** ACM CCS, Nov. 2002.

[11] Roger Dingledine, Nick Mathewson, and Paul Syverson, "**Tor: The Second-Generation Onion Router**," USENIX Security Symposium, Aug. 2004.

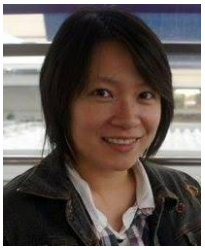
[12] Li Zhuang, Feng Zhou, Ben Y. Zhao, and Antony Rowstron, **"Cashmere: Resilient Anonymous Routing,"** 2nd USENIX Symposium on Networked Systems Design and Implementation (NSDI), 2005.

[13] Aameek Singh, Bugra Gedik, Ling Liu, **"Agyaat: Mutual Anonymity over Structured P2P Networks,"** In Emerald Internet Research Journal (Special Issue on Privacy and Anonymity in the Digital Era), VOL. 16, ISSUE 2, 2006.

[14] Stevens Le Blond, et al., **"Towards Efficient Traffic-Analysis Resistant Anonymity Networks,"** in Proc. of Proceedings of the ACM SIGCOMM 2013, PP. 303-314.

[15] Sahai and B. Waters, **"Fuzzy Identity-Based Encryption,"** In Eurocrypt 2005, LNCS 3494, pp. 457-473, Springer-Verlag, 2005.

AUTHOR BIOGRAPHY



Chia-Chen Wu received her M.S. degree in computer science from the Computer Science Department at National Chiao-Tung University in 2008. She is interested in routing security, elliptic curve cryptography. Contact her at chiachen.cs95g@gmail.com

Yu-Lun Huang received the B.S., and Ph.D. degrees in Computer Science, and Information Engineering from the National Chiao-Tung University, Taiwan in 1995, and 2001, respectively. She has been a member of Phi Tau Phi Society since 1995. She is now an associate professor in the Department of Electrical & Computer Engineering of National Chiao-Tung University (NCTU). She is now the Associate Dean of NCTU Academic Affairs, Director of Center for Continuing Education and Training at NCTU, and Director of Center for Teaching and Learning Development at NCTU. She has been serving the Secretary General of Taiwan Open Course Consortium since 2014. Her research interests include wireless security, virtualization security, embedded software, embedded operating systems, risk assessment, secure payment systems, VoIP, QoS and critical information infrastructure protection (CIIP), IoT Security, LTE Security, creative and innovative teaching model, etc.

Shiuhpyng Shieh received the M.S. and Ph.D. degrees in electrical and computer engineering from the University of Maryland, College Park, respectively. He is a distinguished professor and past chair of the Department of Computer Science, NCTU; and the Director the Taiwan Information Security Center at NCTU. He is an IEEE fellow and ACM Distinguished Scientist. Dr. Shieh is a Senior Member of IEEE, a steering committee member of ACM SIGSAC, and an editor of IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Reliability, Journal of Computer Security, and is also a former editor of ACM Transactions on Information and System Security, IEEE Internet Computing, and Journal of Information Science and Engineering. Contact him at ssp@cs.nctu.edu.tw