National Conference on Advances in Computer Science and Applications with International Journal of Computer Applications (NCACSA 2012)
Proceedings published in International Journal of Computer Applications® (IJCA)

Secure Multipath Data Routing using Cloud Platform

K.Radhika
Lecturer of Computer Science Department
Tamil Nadu college of Engineering

ABSTRACT
The concept behind secure data collection using randomized dispersive routes used for preventing compromised node and denial of service attacks. These two attacks are familiar for generating black holes during passive interception and information block delivery. A randomized path delivery for secure and reliable data collection in wireless sensor networks was designed to generate highly randomized dispersive routes at low energy cost and by reducing the unnecessary retransmissions and improve energy efficiency. Besides randomness, the generated routes are evolved using two propagation techniques NRRP & DRP so as to achieve energy consumption under given security constraints without generating extra copies of secret shares. In this paper, we propose to implement cloud platform, a third party onsite (TPO) and a third party field (TPF). Afore said proposal shall increase the agility of the concept and shall eliminate the drawbacks of existing concept.

Keywords

TPO, TPF, Propagation Schemes, Multipath routes.

1. INTRODUCTION
Cloud computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows end users and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth. One of the biggest concerns with cloud data storage is that of data integrity verification at entrusted servers. For example, the storage service provider, which experiences Byzantine failures occasionally, may decide to hide the data errors from the clients for the benefit of their own. To ensure the correctness of data, we consider the task of allowing a third party onsite (TPO), a third party field (TPF), on behalf of the cloud client. While the former audits the integrity of packets in cloud storage server and adapting one among two propagation phases for packets. While the later audits the integrity of packets received, efficiency of routing nodes and encrypting packets for destination routing. Allowing such auditing entities at different stages of packet routing makes it multi-authentication and packet integrity verification till destination routing more efficient.

2. EXISTING SYSTEM
Instead of selecting paths from a pre-computed set of routes, randomized multipath routing algorithm computes multiple paths in a randomized way each time an information packet need to be sent, such that the set of routes taken by various shares of different packets keep changing over time. As a result, a large number of routes can be potentially generated for each source and destination. To intercept different packets, the adversary has to compromise or jam all possible routes from the source to the destination, which is practically infeasible. Because routes are now randomly generated, they may no longer be node-disjoint.

However, the randomized multipath routing algorithm ensures that the randomly generated routes are as dispersive as possible, i.e., the routes are geographically separated as far as possible such that they have high likelihood of not simultaneously passing through a black hole. Considering the stringent constraint on energy consumption in WSNs, the main challenge in our design is to generate highly dispersive random routes at low energy cost. As explained later, such a challenge is not trivial. Due to security considerations, we also require that the route computation be implemented in a distributed way, such that the final route represents the aggregate decision of all the nodes participating in the route selection. As a result, a small number of colluding/compromised nodes cannot dominate the selection result. In addition, for efficiency purposes, we also require that the randomized route selection algorithm only incurs a small amount of communication overhead.

When a sensor node wants to send a packet to the sink, it first breaks the packet into M shares according to a (T, M)-threshold secret sharing algorithm, e.g., the Shamir's algorithm. Each share is then transmitted to some randomly picked neighbour. That neighbour will continue to relay the share it has received to other randomly picked neighbours, and so on. In each information share, there is a TTL field, whose initial value is set by the source node to control the total number of randomized relays. After each relay, the TTL field is reduced by 1. When the TTL count reaches 0, the final node receiving this share stops the random propagation phase and begins to route this share towards the sink using normal single-path routing. Once the sink collects at least T shares, it can inversely compute the original information. No information can be recovered from less than T shares. Because routes are randomly generated, there is no guarantee that different routes are still node-disjoint. However, the algorithm should ensure that the randomly generated routes are as dispersive as possible, i.e., different routes are geographically separated as far as possible such that they have high likelihood of not simultaneously passing through a black hole. Considering the stringent requirement on energy consumptions in WSNs, the major challenge in our design is to generate highly dispersive random routes at low energy cost. As explained later, such a challenge is not trivial. Due to security considerations, we also require that the route computation be implemented in a distributed way, such that the final route represents the aggregate decision of all the nodes participating in route selection. As a result, a small number of colluding/compromised nodes cannot dominate the selection result. In addition, for efficiency purposes, the randomized route selection algorithm only incurs a small amount of communication overhead. The above proposed system is implemented in a three step process which was explained below.

2.1 SENDER

Sender is a small and simple application that connects to a port through protocol and then sends text strings to destination using IP address and port. Each and every client wants to know port number of the receiver and IP address of the receiver. There are two options for sending a packet. One is normal mode and another one is traffic mode. By knowing the details about which file we send it including file size, modified time, file property and etc with or without acknowledgment for receiving.

2.2 RANDOMIZED MULTIPATH DELIVERY

2.2.1 MULTIPATH ROUTER

Consider the delivery of a packet with the destination at a node. In order to minimize the probability that packets are eavesdropped over a specific link, a randomization process for packet deliveries is adopted. In this process, the previous next hop for the source node is identified. Then, the process randomly picks up a neighboring node excluding already selected hop as the next hop for the current packet transmission. The exclusion of previous selected hop for the next hop selection avoids transmitting two consecutive packets in the same link, and the randomized pickup prevents attackers from easily predicting routing paths for the coming transmitted packets. The number of entries in the history record for packet deliveries to destination nodes. In order to efficiently look up the history record for a destination node, we maintain the history record for each node in a hash table. Before the current packet is sent to its destination node, we must randomly pick up a neighboring node excluding the used node for the previous packet.

2.3 NON-REPETITIVE RANDOM PROPAGATION

NRRP is based on PRP, but it improves the propagation efficiency by recording all the nodes that the propagation has traversed so far. More specifically, NRRP adds a "node-in-route" (NIR) field to the header of each share. Initially, this field is empty. Starting from the source node, whenever a node propagates the share to the next hop, the id of the up-stream node is appended to the share's NIR field. Nodes included in NIR are excluded from the random pick of the next hop of propagation. This non repetitive propagation guarantees that the share will be relayed to a different node in each step of random propagation, leading to better propagation efficiency.

2.4 DIRECTED RANDOM PROPAGATION

DRP improves the propagation efficiency by using two-hop neighbourhood information. More specifically, DRP adds a "last-hop neighbour list" (LHNL) field to the header of each share. Before a share is propagated to the next node, the relaying node first replaces the old content in the LHNL field of the share by its neighbour list. When the next node receives the share, it compares the LHNL field against its own neighbour list, and randomly picks one node from its neighbours that are not in the LHNL. It then decrements the TTL value, updates the LHNL field, and relays the share to the next hop, and so on. Whenever the LHNL fully overlaps with or contains the relaying node's neighbour list, a random neighbour is drawn, According to this propagation method; DRP reduces the chance of propagating a share back and forth by eliminating this type of propagation within any two immediate consecutive steps. Compared with PRP, DRP it leads to better propagation efficiency for a given TTL value.

2.5 RECEIVER

Receiver receives the incoming packets from sender via router. Here want to access that source IP address, destination IP address, source port, destination port. It is act as a receiver. First we want to do set a receiving path in our receiver. Receiving folder receive the files from the clients. Here we have only one receiver. All clients files are receive here. We want to refresh receiver to get an incoming packets. The incoming packets are sometimes may be damaged or not received from clients then the receiver send the acknowledgment to client. By calculating the time delay of the incoming packets and the time delay value display in client or server module.

2.6 DRAWBACKS

- The adversary can selectively compromise nodes; the sensed information is intercepted in each fixed routing path even if it can be distributed over different routes. The integrity of data was not maintained throughout the data transmission.

- The adversary can still intercept part of information; we reduce the probability of interception to an acceptable extent. Thus, malicious node may participate with fake identities to several paths, rendering multipath routing insecure.

- During route request propagation, each node receives request appends it neighbourhood information along with RC4 encryption and broadcasts it with previously received information. This greatly increases the message size.

3. PROPOSED SYSTEM

In the cloud paradigm, three different network entities such as client, cloud service provider and cloud storage server has been identified. The client entity which routes packets to end-user based elasticity via-dynamic and relies on the cloud for packet maintenance and computation. Cloud service provider (CSP) has significant storage space and computation resource to maintain client's and end user's data; Cloud storage server entity is used to manage the packets demanded by the end user. Third party onsite (TPO) which has expertise and capabilities that clients do not posses has been entrusted to assess the risk during packet routing elasticity via-dynamic by client and end-user. Third party onsite (TPO) selects the neighbouring third party field (TPF) for end-user destination. TPO randomly selects neighbouring nodes for TPF and adapts suitable propagation phase accordingly. TPF receives the packets; assess the efficiency of routing neighbouring nodes and assigns TTL field. TPF do not accept anymore packets from the same nodes for simultaneous packet routing. TPF encrypts packets and generates key for the same. Encrypted packets shall be sent to destination of the end-user and the key shall be sent to end-user mobile.

3.1 ADVANTAGES

- The end user can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each server.
- Provides highly dispersive random routes at low energy cost without generating extra copies of secrete shares. If the routing algorithm becomes known to the adversary, the adversary still cannot pinpoint the routes traversed by each packet. Energy efficient.
- Multi-authentication and packet integrity verification ensures loss less routing of packets from packet to end-user.
- Maintenance cost is reduced as a third party maintains everything from running the cloud to packet routing.

4. PROJECT OVERVIEW

In this proposed concept, the end user was requested some packets from clients' cloud; the cloud collects packets based on end-users' request and send them to the Third Party Onsite (TPO). Third party onsite (TPO) selects the neighbouring third party field (TPF) for end-user destination. Packets are sent as dispersive possible by adapting one of the two propagation phases, Directed Random Propagation (DRP) and Non-Repetitive Random Propagation (NRRP) through neighbouring nodes for TPF. TPF receives the packets; assess the efficiency of routing neighbouring nodes and assigns TTL field. TPF do not accept anymore packets from the same nodes for simultaneous packet routing. TPF encrypts packets and generates key for the same. Encrypted packets shall be sent to destination of the end-user and the key shall be sent to end-user mobile.

4.1 THIRD PARTY ONSITE (TPO)

The third party onsite (TPO) is an onsite auditing and packet routing server. TPO is introduced as a measure to ensure integrity of packets stored in cloud and ensures that packets are sent as dispersive possible by adapting one of the two propagation phases, Directed Random Propagation (DRP) and Non-Repetitive Random Propagation (NRRP) through neighbouring nodes for TPF. TPF is selected based on its proximity to end-user destination for packets delivery. Users rely on the CS for cloud packets storage and maintenance. They may also dynamically interact with the CS to access and update their stored packets for various application purposes. The users may resort to TPO for ensuring the storage security of their outsourced packets, while hoping to keep their packets private from TPO. However, during providing the cloud packets storage based services, for their own benefits the CS might neglect to keep or deliberately delete rarely accessed packets which belong to ordinary cloud users. Moreover, the CS may decide to hide the data corruptions caused by server hacks or Byzantine failures to maintain reputation. TPO should be able to efficiently audit the cloud data storage without local copy of data and without bringing in additional on-line burden to cloud users.

4.2 THIRD PARTY FIELD (TPF)

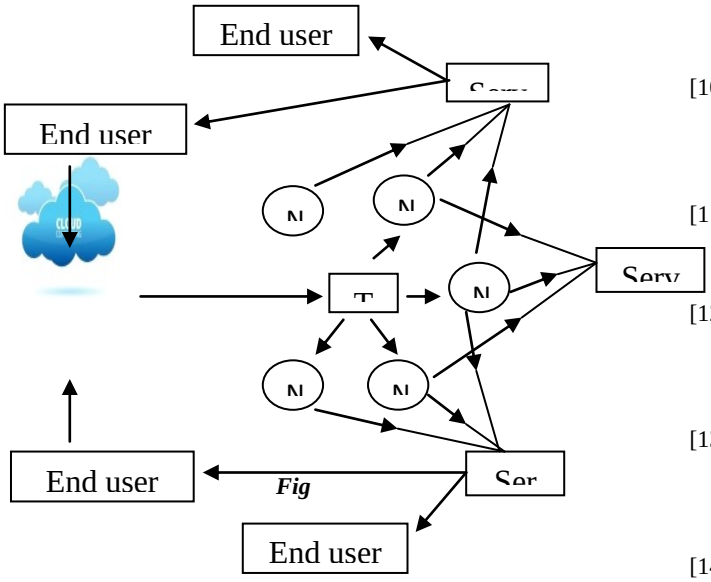
Third party field (TPF) is an auditing, encrypting and routing server located in field. TPF is selected by TPO based on its proximity to end-user destination for packets delivery. TPF is introduced as a measure to ensure integrity of packets received from nodes and assess the efficiency of routing neighbouring nodes and assigns TTL field. TPF do not accept anymore packets from the same nodes for simultaneous packet routing. TPF encrypts packets and generates key for the same. Encrypted packets shall be sent to destination of the end-user and the key shall be sent to end-user mobile. Users rely on TPF to prevent a compromised node routing malicious packets to destination, nodes routing packets are informed by TPO to TPF prior to routing.

5. SYSTEM IMPLEMENTATION

In this proposed concept, the end user was requested some packets from clients' cloud; the cloud collects packets based on end-users' request and send them to the Third Party Onsite (TPO). Third party onsite (TPO) selects the neighbouring third party field (TPF) for end-user destination. Packets are sent as dispersive possible by adapting one of the two propagation phases, Directed Random Propagation (DRP) and Non-Repetitive Random Propagation (NRRP) through neighbouring nodes for TPF. TPF receives the packets; assess the efficiency of routing neighbouring nodes and assigns TTL field. TPF do not accept anymore packets from the same nodes for simultaneous packet routing. TPF encrypts packets and generates key for the same. Encrypted packets shall be sent to destination of the end-user and the key shall be sent to end-user mobile. The third party onsite (TPO) is an onsite auditing and packet routing server. TPO is introduced as a measure to ensure integrity of packets stored in cloud and ensures that packets are sent as dispersive possible by adapting one of the two propagation phases, Directed Random Propagation (DRP) and Non-Repetitive Random Propagation (NRRP) through neighbouring nodes for TPF. TPF is selected based on its proximity to end-user destination for packets delivery. Users rely on the CS for cloud packets storage and maintenance. They may also dynamically interact with the CS to access and update their stored packets for various application purposes. The users may resort to TPO for ensuring the storage security of their outsourced packets, while hoping to keep their packets private from TPO. However, during providing the cloud packets storage based services, for their own benefits the CS might neglect to keep or deliberately delete rarely accessed packets which belong to ordinary cloud users. Moreover, the CS may decide to hide the data corruptions caused by server hacks or Byzantine failures to maintain reputation. TPO should be able to efficiently audit the cloud data storage without local copy of data and without bringing in additional on-line burden to cloud users. TPO is introduced as a measure to ensure integrity of packets stored in cloud and ensures that packets are sent as dispersive possible by adapting one of the two propagation phases, Directed Random Propagation (DRP) and Non-Repetitive Random Propagation (NRRP) through neighbouring nodes for TPF. TPF is selected based on its proximity to end-user destination for packets delivery. Users rely on the CS for cloud packets storage and maintenance. They may also dynamically interact with the CS to access and update their stored packets for various application purposes. The users may resort to TPO for ensuring the storage security of their outsourced packets, while hoping to keep their packets private from TPO.

However, during providing the cloud packets storage based services, for their own benefits the CS might neglect to keep or deliberately delete rarely accessed packets which belong to ordinary cloud users. Moreover, the CS may decide to hide the data corruptions caused by server hacks or Byzantine failures to maintain reputation. TPO should be able to efficiently audit the cloud data storage without local copy of data and without bringing in additional on-line burden to cloud users. TPF encrypts packets and generates key for the same. Encrypted packets shall be sent to destination of the end-user and the key shall be sent to end-user mobile. Users rely on TPF to prevent a compromised node routing malicious packets to destination, nodes routing packets are informed by TPO to TPF prior to routing.

Multipath random secure data routing become more agile and automated by implementing the concept over cloud platform. Inclusion of third party onsite (TPO) and third party field (TPF) entities was instrumental in verifying the integrity of packets routed from cloud to end-user destination.



Fig

5.1 System architecture

6. FUTURE ENHANCEMENTS

We propose to use open source software as platform for implementing multicast-tree propagation along with direct random propagation and non-repetitive random propagation. Updating third party onsite and third party field regarding friendly neighbouring nodes elasticity via-dynamic for efficient and secure packet routing.

7. RFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A Survey on Sensor Networks,” IEEE Comm. Magazine, vol. 40, no. 8, pp. 102-114, Aug. 2002.

[2] Cong Wang,Qian Wang,Kui Ren,Wenjing Lou (2010),"Privacy Preserving Public Auditing for Data Storage Security in Cloud Computing".

[3] A. L. Ferrara, M. Greeny, S. Hohenberger, M. Pedersen (2009), "Practical short signature batch verification", in Proceedings of CT-RSA, volume 5473 of LNCS. Springer-Verlag, pp. 309–324.

[4] H. Shacham, B. Waters (Dec 2008), "Compact proofs of retrievability", in Proc. of Asiacrypt 2008, vol. 5350, pp. 90–107

[5] M.A.Shah, R.Swaminathan, M. Baker (2008), "Privacy preserving audit and extraction of digital contents",Cryptology ePrint Archive.

[6] Q. Wang, C. Wang, J. Li, K. Ren, W. Lou (2009), "Enabling public verifiability and data dynamics for storage security in cloud computing", in Proc. of ESORICS’09, Saint Malo.

[7] Wang, K. Ren, W. Lou (2010), “Achieving secure, scalable, and fine-grained access control in cloud computing”, in Proc. of IEEE INFOCOM’10, San Diego, CA, USA.

[8] C.L. Barrett, S.J. Eidenbenz, L. Kroc, M. Marathe, and J.P. Smith, “Parametric Probabilistic Sensor Network Routing,” Proc. ACM Int’l Conf. Wireless Sensor Networks and Applications (WSNA), pp. 122-131, 2003.

[9] M. Burmester and T.V. Le, “Secure Multipath Communication in Mobile Ad Hoc Networks,” Proc. Int’l Conf. formation Technology: Coding and Computing, pp. 405-409, 2004.

[10] W. Lou and Y. Kwon, “H-Spread: A Hybrid Multipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks,” IEEE Trans. Vehicular Technology, vol. 55, no. 4, pp. 1320- 1330, July 2006.

[11] W. Lou, W. Liu, and Y. Fang, “Spread: Enhancing Data Confidentiality in Mobile Ad Hoc Networks,” Proc. IEEE INFOCOM, vol. 4, pp. 2404-2413, Mar. 2004.

[12] R. Mavropodi, P. Kotzanikolaou, and C. Douligeris, “SecMR—a Secure Multipath Routing Protocol for Ad Hoc Networks,” Ad Hoc Networks, vol. 5, no. 1, pp. 87-99, Jan. 2007.

[13] B. Vaidya, J.Y. Pyun, J.A. Park, and S.J. Han, “Secure Multipath Routing Scheme for Mobil e Ad Hoc Network,” Proc. IEEE Int’l Symp. Dependable, Autonomic and Secure Computing, pp. 163-171, 2007.

[14] A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, M. Zaharia, “Above the clouds: A berkeley view of cloud computing,” University of California, Berkeley, Tech. Rep, 2009.

[15] Cong Wang,Qian Wang,Kui Ren,Wenjing Lou (2009),"Ensuring Data Storage Security in Cloud Computing".

8. AUTHORS PROFILE

K.Radhika, I have completed my Bachelor’s degree Computer Science & Engineering in Anna University, Chennai. I have completed my Master’s Degree in Computer Science & Engineering in Anna university, Coimbatore .