International Journal of Research
Available at
https://www.internationaljournalofresearch.org/
ISSN: 2236-6124
Volume 09 Issue 01
Jan-June 2019

Building Confidential and Efficient Query Services in the Cloud with Rasp Data Perturbation

[1]G LAKSHMI VARA PRASAD, M.Tech, [2]Thammisetty Sunil Kumar

[1]Assistant Professor Department of CSE, Qis College of Engineering and Technology , Ongole, PrakasamDist,Andhra Pradesh

[2]PG Scholar,Dept of CSE, QIS College of Engineering and Technology Ongole ,PrakasamDist,Andhra Pradesh

Abstract- With the wide deployment of public cloud computing infrastructures, using clouds to host data query services has become an appealing solution for the advantages on scalability and cost-saving. However, some data might be sensitive that the data owner does not want to move to the cloud unless the data confidentiality and query privacy are guaranteed. On the other hand, a secured query service should still provide efficient query processing and significantly reduce the in-house workload to fully realize the benefits of cloud computing. We propose the random space perturbation (RASP) data perturbation method to provide secure and efficient range query and kNN query services for protected data in the cloud. The RASP data perturbation method combines order preserving encryption, dimensionality expansion, random noise injection, and random projection, to provide strong resilience to attacks on the perturbed data and queries. It also preserves multidimensional ranges, which allows existing indexing techniques to be applied to speedup range query processing. The kNN-R algorithm is designed to work with the RASP range query algorithm to process the kNN queries. We have carefully analyzed the attacks on data and queries under a precisely defined threat model and realistic security assumptions. Extensive experiments have been conducted to show the advantages of this approach on efficiency and security.

I.Introduction

Mobile Ad hoc NETwork (MANET) is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. MANET structure may vary depending on its application from a small, static network that is highly power constrained to a large-scale, mobile, highly dynamic network. Every node works both a transmitter and a receiver. Nodes communicate directly with each other when they are both within the same communication range. Otherwise, they rely on their neighbors to relay messages. Industrial remote access and control via wireless networks are becoming more and more popular these days. One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their

mobility. This communication is limited to the range of transmitters. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own. MANET solves this problem by allowing intermediate nodes to rely data transmission. There are two types of MANETs: closed and open. In a closed MANET, all mobile nodes cooperate with each other toward a common goal, such as emergency search/rescue or military and law enforcement operations. In an open MANET, different mobile nodes with different goals share their resources in order to ensure global connectivity. Some resources are consumed quickly as the nodes participate in the functions. Battery power is considered to be more importance in a mobile environment. An individual mobile node may attempt to benefit from other nodes, but refuse to share its own resources. Such nodes are called selfish or misbehaving nodes and their behaviour is termed selfishness or misbehaviour. A selfish node may refuse to forward the data it received to save its own energy. MANET has two types of network, namely single-hop and multi-hop [1]. In a single-hop network, all nodes within the same radio range communicate directly with each other. In a multi-hop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range. A mobile ad-hoc network is a self-configuring network of mobile routers (and associated hosts) connected by wireless links - the union of which form a random topology. The routers are free to move randomly and organize themselves at random; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet. Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like military conflicts, emergency medical situations. However, the open medium of MANET is vulnerable to various types of attacks. For example, due to the nodes' lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks. Attackers can easily insert the malicious or incorporate nodes into the network to achieve attacks. Such misbehaving nodes need to be detected so that these nodes can be avoided by well behaved nodes. Many schemes and intrusion detection systems proposed to detect such nodes.

II. Related Work

Due to the limitation of most MANET routing protocol, nodes in MANETs assume that other nodes always cooperate with each other to relay data. This assumption leaves the attackers with the opportunities to achieve significant on the network with just one or two compromised nodes. To address this drawback, IDS should be added to enhance the security level of MANETs. If MANET can detect the attackers as soon as they enter the network, we will be able to describe three existing approaches, namely, Watchdog, TWOACK, and Adaptive Acknowledgement. the Watchdog scheme is consisted of two elements, namely, Watchdog and Pathrater. Watchdog detects malicious misbehaviors by promiscuously being attentive to its next hop's transmission. If a watchdog node overhears that its next node fails to forward the packet among a particular amount of your time, it will increase its failure counter. Whenever a node's failure counter exceeds a predefined threshold, the Watchdog node reports it as misbehaving. Moreover, compared to

ISSN: 2236-6124
Volume 09 Issue 01
Jan-June 2019

another schemes, Watchdog is capable of police investigation malicious nodes instead of links.

TWOACK: With respect to the six weaknesses of the Watchdog theme, several researches projected new approaches to unravel these problems. TWOACK detects misbehaving links by acknowledging each information packet transmitted over each three consecutive nodes on the trail from the supply to the destination. TWOACK is needed to figure on routing protocols like Dynamic SupplyRouting. The operating method of TWOACK is shown in Fig. 1: Node A primary forwards Packet 1 to node B, and then, node B forwards Packet 1 to node C. Once node C receives Packet 1, because it is two hops from node A, node C is duty-bound to come up with a TWOACK packet, that contains reverse route from node A to node C, and sends it back to node A. The retrieval of this TWOACK packet at node A indicates that the transmission of packet one from node A to node C is fortunate. Otherwise, if this TWOACK packet is not received in an exceedingly predefined period, each nodes B and C area unit reported malicious. Identical method applies to each three consecutive nodes on the remainder of the route.

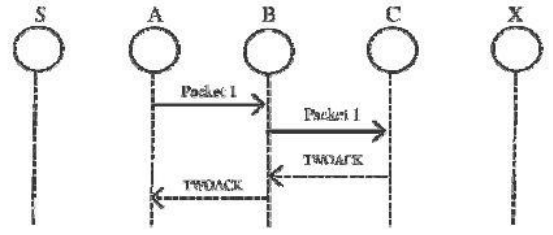

Fig1. Each node is required to send back an acknowledgment packet to the node that is two hops

Many historical events have shown that intrusion prevention techniques alone, such as encryption and authentication, which are usually a first line of defense, are not sufficient. As the system become more complex, there are also more weaknesses, which lead to more security problems. Intrusion detection can be used as a second wall of defense to protect the network from such problems. If the intrusion is detected, a response can be initiated to prevent or minimize damage to the system. Some assumptions are made in order for intrusion detection systems to work [1]. The ¯rst assumption is that user and program activities are observable. The second assumption, which is more important, is that normal and intrusive activities must have distinct behaviors, as intrusion detection must capture and analyze system activity to determine if the system is under attack.

III. A Secure Intrusion Detection System for MANET

MANET does not require a fixed network infrastructure; every single node works as both a transmitter and a receiver. Nodes communicate directly with each other when they are both within the same communication range [2]. Otherwise, they rely on their neighbors to relay messages. The self-configuring ability of nodes in MANET made it popular among critical mission applications like military use or emergency recovery. The open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. In this case, it is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks. In this paper it proposes a new system called EAACK-Enhanced Adaptive Acknowledgement is specially designed for MANETs to detect the attackers. EAACK is an

acknowledgement based scheme. EAACK is an acknowledgment-based IDS. This scheme makes use of digital signature. It requires all acknowledgment packets to be digitally signed. This new system requires acknowledgement for the every packet sent to the receiver with the signature. First after sending packets to the receiver it waits for the acknowledgement. Within the predefined time interval the source received the acknowledgement from receiver then the packet transmission is successful. Otherwise the source node will switch to the secure acknowledgement mode. In secure acknowledgement mode every consecutive three nodes work together to detect the misbehaving nodes in the route. Every third node in the group needs to give acknowledgement to the first node. If any node fails to send acknowledgement is marked as malicious node. Then the source node switches to misbehavior report authentication (MRA) mode. In MRA mode, source node first searches its local knowledge base for the alternative path to the destination. Upon receiving MRA packet, destination node will searches for any received MRA is stored; if it stored then ignore the new packet and the node which sends that packet marked as malicious. Otherwise the nodes marked as malicious in the packet are removed from the route in future transmission. This system uses the digital signatures to authenticate the acknowledgement packets. Digital signatures prevent the acknowledgement packets to be forged. The sender of the acknowledgement packet must sign the packet and after the reception of the packet receiver will verify the authenticity of the packet. This new system reduces the packet dropping attack; it is the major security threat. In case of limited transmission power, receiver collision, false misbehavior rate EAACK is a preferred IDS than the existing approaches.

IV. Enhanced Intrusion Detection Systems for Discovering Malicious Nodes in Mobile Ad Hoc Network

In this paper a new intrusion detection system is proposed called ExWatchdog system to overcome the weakness of watchdog system. ExWatchdog is an extension of Watchdog and its function is also detecting intrusion from malicious nodes and reports this information to the response system, Route guard. It aims to detect nodes that falsely report other nodes as misbehaving. ExWatchdog has two parts: Watchdog and routeguard. Either in watchdog or route guard, each node updates ratings of nodes it knows according to the information provided by any node in the network. If a node send a false report that says other nodes as misbehaving. A malicious node could partition the network by claiming that some nodes following it in the path are misbehaving. ExWatchdog detection system solve this problem. The source node first searches a path that has no malicious node in it from the routing table. If there is not such a path available, the source then launch a Route Discovery to find a new one. After finding a path, the source sends the message using the found path. Upon receiving the message, destination node will search its own table to see if there is a match. If there is not a matching entry in the table, it means the node is malicious and the destination node returns a message to the source confirming that the malicious node is really malicious. If there is, destination node then compares the sum field of the passing in message with the one found in the table. If the two sums equal, it means that the malicious node

forwards all packets that the source sends thus it is not malicious. On the contrary, if the two sums are not equal, the node falsely report might be malicious. Routeguard will use this information to update the rating of corresponding node. It discovers malicious nodes which can partition the network by falsely reporting other nodes as misbehaving and then proceeds to protect the network. The main feature of the proposed system is its ability to discover malicious nodes which can partition the network by falsely reporting other nodes as misbehaving and then proceeds to protect the network.

V. Detecting Forged Acknowledgements in Manet

MANET suffers from the threat that it fails to detect misbehaving node when the attackers are smart enough to forge the acknowledgement packets. In this paper, we introduce a intrusion detection scheme with digital signature algorithm to provide secure transmission against false misbehavior report and partial dropping. This intrusion detection system assumes the link between in the network is bidirectional. Misbehaving nodes also lies in the network. It assumes misbehaving nodes are intermediate nodes; they are neither the source node nor the destination node. In routing stage they cooperate with other nodes but they drop the packets instead of forwarding to next node. After dropping the packets the misbehaving node generate a forge acknowledgement and sent to source node in order to conceive the source node. When the source node sends out the data packet it registers the packet ID and sent time. After receiving packet destination node need to send acknowledgement packet with packet id to source. Successful reception of acknowledgement packet at source the transmission is completed and confirmed. After certain time period the source node does not receive the acknowledgement from destination it switch to secure acknowledge mode. In this scheme, for every three consecutive nodes along the transmission route, the third node is required to send back an S-ACK packet back to the first node to confirm receiving the packet. In this system the third node is required to sign this S-ACK packet with its own digital signature. The intention of doing this is to prevent the second node from forging the S-ACK packet without forward the packet to the third node. This is really dangerous as the malicious node can create a black-hole in the network without being detected. When the first node receives this S-ACK packet, it verifies the third node's signature with the redistributed public key. On the other hand, if no S-ACK packet is received within a predefined time period; the first node will report both second node and the third node as malicious. When the source node receives the malicious report, instead of trusting the report immediately and marks the nodes as malicious, it requires the source node to switch to MRA mode to confirm. The source node switches to MRA mode by sending out an MRA packet to the destination node via a different route. If such route does not exist in the cache, the source will find a new route. For extreme conditions when there are no alternative routes from source node to the destination node, this detection system, by default, accepts the misbehaving report.

VI. Routing Misbehavior Detection

In semiautonomous mobile sensor networks, since human operators may be involved in the control loop, particular improper actions may cause accidents and result in catastrophes. For such systems, this paper proposes a command filtering framework to accept or reject the human-issued commands

so that undesirable executions are never performed. In the present approach, Petri nets are used to model the operated behaviors and to synthesize the command filters for supervision. This paper proposes the 2ACK scheme that serves as an add-on technique for routing schemes to detect routing misbehaviour and to mitigate their adverse effect. It is used to detect some selfish nodes will participate in the route discovery and maintenance processes but refuse to forward data packets. 2ACK scheme send two-hop acknowledgment packets in the opposite direction of the routing path. It is a network-layer technique to detect misbehaving links rather than nodes and to mitigate their effects. The 2ACK scheme detects misbehavior through the use of a new type of acknowledgment packet, termed 2ACK. A 2ACK packet is assigned a fixed route of two hops (three nodes) in the opposite direction of the data traffic route. 2ACK transmission takes place for every set of triplets along the route. Therefore, only the first router from the source will not serve as a 2ACK packet sender. The last router just before the destination and the destination will not serve as 2ACK receivers. To reduce additional routing overhead only a fraction of the received data packets are acknowledged in the 2ACK scheme. TWOACK detects misbehaving links by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the destination. Upon retrieval of a packet, each node along the route is required to send back an acknowledgment packet to the node that is two hops away from it down the route. Source send data packet to receiver. Receiver generates the 2ACK packet back to sender. Retrieval of 2ACK packet within a predefined time period indicates successful transmission otherwise both destination and intermediate nodes are reported as malicious.

VII. Conclusion

In this paper Packet-dropping attack has always been a major threat to the security in MANETs. the overview of various intrusion detection systems to detect the malicious nodes and analyze the attacks in the network and provide security against those attacks in order to provide efficient packet transmission without modification, dropping and partial dropping of packets using an efficient intrusion detection system. Our proposed system first sends data packet; if it detects any misbehavior in the network it will find the misbehaving node and eliminate the node from the route. Otherwise it will select the alternate route from its local knowledgebase and start sending packet. This system performs well in presence of false misbehavior reports compared to other intrusion detection system and also reduce the packet dropping.

References

[1] G. Jayakumar and G. Gopinath, ―Ad hoc mobile wireless networks routing protocol—A review,‖ *Journal of Computer Science* ., vol. 3, no. 8, pp. 574–582, 2007.

[2] A. Mishra, K. Nadkarni, and A. Patcha, \Intrusion Detection in Wire-
less Ad Hoc Networks," *IEEE Wireless Communications*, Vol. 11, Issue
1, pp. 48-60, February 2004.

[3] P. Albers, O. Camp, J. Percher, B. Jouga, L. M, and R. Puttini, \Secu-
rity in Ad Hoc Networks: a General Intrusion Detection Architecture
Enhancing Trust Based Approaches," *Proceedings of the 1st Interna-
tional Workshop on Wireless Information Systems (WIS-2002)*, pp. 1-
12, April 2002.

[4] O. Kachirski and R. Guha, \E®ective Intrusion Detection Using Multi-
ple Sensors in Wireless Ad Hoc Networks," *Proceedings of the 36th An-
nual Hawaii International Conference on System Sciences (HICSS'03)*,
p. 57.1, January 2003.
[5] S. Marti, T. J. Giuli, K. Lai, and M. Baker, \Mitigating Routing Mis-
behavior in Mobile Ad Hoc Networks," *Proceedings of the 6th Annual
International Conference on Mobile Computing and Networking (Mo-
biCom'00)*, pp. 255-265, August 2000.
[6] S. Buchegger and J. Le Boudec, \Performance Analysis of the CONFI-
DANT Protocol (Cooperation Of Nodes - Fairness In Dynamic Ad-hoc
NeTworks)," *Proceedings of the 3rd ACM International Symposium on
Mobile Ad Hoc Networking and Computing (MobiHoc'02)*, pp. 226-336,
June 2002.
[7] P. Michiardi and R. Molva, \Core: A Collaborative Reputation mech-
anism to enforce node cooperation in Mobile Ad Hoc Networks," *Com-
munication and Multimedia Security Conference (CMS'02)*, September
2002.
[8] D. B. Johnson, and D. A. Maltz, \The Dynamic Source Routing Pro-
tocol for Mobile Ad Hoc Networks (Internet-Draft)," *Mobile Ad-hoc
Network (MANET) Working Group, IETF*, October 1999.
[9] P. Brutch and C. Ko, \Challenges in Intrusion Detection for Wireless
Ad-hoc Networks," *Proceedings of 2003 Symposium on Applications and
the Internet Workshop*, pp. 368-373, January 2003.
[10] M. G. Zapata, \Secure Ad Hoc On-Demand Distance Vector (SAODV)
Routing," *ACM Mobile Computing and Communication Review
(MC2R)*, Vol. 6, No. 3, pp. 106-107, July 2002.

[11] Y. Hu, D. B. Johnson, and A. Perrig, \SEAD: Secure E±cient Distance
Vector Routing for Mobile Wireless Ad Hoc Networks," *Proceedings of
the 4th IEEE Workshop on Mobile Computing Systems and Applica-
tions (WMCSA'02)*, pp. 3-13, June 2002.
[12] Y. Hu, A. Perrig, and D. B. Johnson, \Ariadne: A secure On-Demand
Routing Protocol for Ad hoc Networks," *Proceedings of the 8th An-
nual International Conference on Mobile Computing and Networking
(MobiCom'02)*, pp. 12-23, September 2002.
[13] A. Perrig, R. Canetti, D. Tygar and D. Song, \The TESLA Broadcast
Authentication Protocol," *RSA CryptoBytes*, 5 (Summer), 2002.
[14] Y. Huang and W. Lee, \A Cooperative Intrusion Detection System for
Ad Hoc Networks," *Proceedings of the ACM Workshop on Security in
Ad Hoc and Sensor Networks (SASN'03)*, pp. 135-147, October 2003.

[15] Elhadi M.Shakshnki , Nan Kang and Tarek R. Sheltami " EAACK – A secure Intrusion Detection System for MANET" IEEE Transaction on Industrial electronics vol 60 . No3 , March 2013.

Author Details:

G LAKSHMI VARA PRASAD,
working as an assistant professor in the department of information technology, qiscet ongole.
I guided 4 M. Tech students and 28 b. Tech students.

ISSN: 2236-6124
Volume 09 Issue 01
Jan-June 2019

Thammisetty Sunil Kumar
B. Tech(CSE) in vignan university, vadlamudi
M. Tech(CSE) Scholar in QIS college of Engg and Tech, Ongole
Building confidential and efficient query services in the cloud with rasp data perturbation