UDC 004.056

S.V. GLADYSH

Norwegian University of Science and Technology, Norway

STRATEGICAL ATACKING ON DATA FORWARDING PLANE OF ROUTING PROTOCOLS WITH BYZANTINE FAILURE ROBUSTNESS

The problem of Byzantine failure robustness of routing protocols is considered. The focus is made on protocol weaknesses on data forwarding plane and strategic Byzantine attacks. Several routing protocols are analyzed, and their limitations are shown. Critical mistakes in the protocols are discovered, and effective attack scenarios are proposed. Existing methodology of protocol designing is criticized.

Key words: *Byzantine failures, Data forwarding, Failure robustness, Intrusion detection, Routing protocols.*

Introduction

A common approach is to distinguish between two planes of routing [1]. Each of these planes might be attacked in a specific way: a) control plane - violations to behave in accordance with routing protocol: lying about a network topology by means of false advertisements and introducing faked links or nodes, black hole, wormhole attacks etc; b) data plane - violations to correctly forward data packets: dropping, selectively dropping, injection, modification, delaying and reordering of data packets.

Most part of research on securing routing protocols were addressed to attacks on control plane. Until the latest few years, the data plane of routing remained less investigated, though it was proven to be no less important than the control plane [2].

Data forwarding misbehavior is possible only for routers which are the "legal" authorized participants of the routing process in the given network. Therefore, in order to misbehave these routers must had been compromised. According to the "Byzantine Generals Problem" [5], data forwarding misbehavior represents a type of Byzantine misbehavior; and correspondingly such a compromised router is called a Byzantine adversary (attacker, node, etc) [3].

1. Challenges of Byzantine robust routing and threats of data forwarding

1.1. Network protocols with Byzantine robustness

The fundamental work, where the problems of *routing with Byzantine robustness* and *the data forwarding plane security* were first raised, is a PhD thesis of R. Perlman [3]. There she first defined *a Byzantine routing failure* as one in which a router instead of halting (as it would in fail-stop failure), continues to operate, but incorrectly, i.e.: a) lies about routing connectivity, for example by advertising fake links or nodes; b) corrupts routing information from other nodes; c) agrees to perform the routing algorithm correctly, but then violates forwarding decisions; d) floods the network with garbage traffic.

Network Layer Protocol with Byzantine Robustness (NPBR) [3] is a link-state routing protocol for traditional wired networks, and consists of two basic types of routing: A.) *Robust flooding* based on source routing along multiple paths, digitally signed route-setup packets, sequence numbers, and reserved buffers. Robust flooding is a method of reliable packet delivery to all correctly operating routers. It was designed for public key distribution and broadcasting link state packets. B.) *Data packets forwarding*, in which the source selects and sets up a path to the destination, including: packet specified forwarding; and forwarding with connection-oriented path setup.

NPBR is resilient against Byzantine failures of trusted nodes and against Byzantine links, but its limitation is that it requires the network to be small enough so that every router could keep state proportional to squared number of nodes. To overcome this Perlman introduced a hierarchical NPBR [4].

In NPBR and hierarchical NPBR many practical implementation issues still require to be developed, such as fault detection and response algorithms.

1.2. Detecting and isolating malicious routers

The problem of detection and isolation of data forwarding misbehavior in traditional wired networks is studied in [2]. The authors surveyed several secure

protocols for the data plane of routing, and classified the data forwarding misbehavior onto the types: a) packet loss; b) packet fabrication; c) packet modification; d) packet reordering; e) time behavior.

In [2] detection of a compromised router is based on deviations from expected behavior and realized by its neighbors. This includes 3 tasks: A.) Traffic validation by using traffic summaries (*Conservation of Flow, Conservation of Content, Conservation of Order*), which should be efficiently (in terms of memory) aggregated by the neighbors. B.) Distributed detection by synchronizing these aggregated traffic summaries (with minimal network overhead) and finding a consensus. C.) Response by removing detected misbehaving routers from the routing tables of correct routers but without unnecessary high impact on network performance (for example, by removing them only along those paths, where these routers had misbehaved).

The given approach might be attractive, because it covers many types of data forwarding attacks (Table 1), and potentially could make less network overhead in comparison to the other approaches such as: acknowledgement schemes, end-to-end reliability mechanisms, per-hop authentication, timeouts, signed packets and reserved buffers.

Table 1

Types of attacks vs. detection principles

Principle / Attack	Conservation of Flow	Conservation of Content	Conservation of Order
loss	+	+	+
fabrication	-	+	+
modification	-	+	+
reordering	-	-	+
delaying	-	-	-

There are a lot of open questions left, which need further detailed research in order to be implemented in practice. In [2] the Traffic Validation Function is considered as a “black box”, but accurate development of this function is a challenging task.

It is not clear how to reduce the storage and computational overheads without loosing in accuracy. Bloom filters and distributed set reconciliation techniques are just mentioned as possible methods, but these need further in-depth investigation, as well as the problem of timing misbehavior.

The response technique is not developed in details. Further accuracy/overhead trade-off optimization research is possible in defining the quantity of path segments a router need to monitor.

In the network model broadcast channels were ignored, which gives no opportunities for applying the given approach to many types of networks.

1.3. Watching for anomalies in transit conservation

WATCHERS (Watching for Anomalies in Transit Conservation) [6, 7] is a protocol for disruptive router detection via analysis of the number of packets entering and exiting a router.

Each router executes WATCHERS at regular intervals in order to identify neighboring routers that misroute traffic and avoid them. The protocol is a bit similar to the previous one in that it also detects and isolates faulty routers basing on a distributed network monitoring approach.

WATCHERS uses as a traffic summary only a Conservation of Flow Principle, and therefore it addresses only packet loss misbehavior. Many of its limitations were shown in [8]. As the previous protocol, WATCHERS doesn’t consider broadcasting and specifics of wireless ad-hoc networks.

1.4. Early detection of message forwarding faults

A theoretical framework for constructing, estimating and comparing of acknowledgement scheme realizations for data forwarding failure detection is proposed in [9]. Two effectiveness criteria are proposed for protocols:

a) time complexity;

b) communication complexity.

Fault detection is based on timeouts for the expected acknowledgments from the destination and (possibly) from some of the intermediate nodes to the source.

The main premise of this approach is that the actual delivery time of a message over a link is usually much smaller than the a priori known upper bound D on that delivery time. By taking advantage of this observation, the authors developed an abstract model for various time-optimal or communication-optimal acknowledgement schemes that detect and locate any faulty link or faulty path segment.

However, this is a theoretical and rather abstract framework. The model is oversimplified in that it considers only sending of one single message via one end-to-end channel.

1.5. Highly secure and efficient routing

A routing protocol with Byzantine robustness and detection properties presented in [10]. Like NPBR

[3, 4], this protocol combines several security mechanisms: source routing, hop-by-hop authentication, reserved buffers, sequence numbers, timeouts, end-to-end reliability mechanisms, fault announcements. The shortcoming of the given approach is its very high owerhead.

2. Effective data forwarding attacks on multi-hop Byzantine robust routing

2.1. On-demand secure Byzantine routing

In [11] presented an on-demand secure routing protocol (ODSBR), which was developed in order to be resilient against Byzantine failures, including colluding Byzantine adversaries. Main ideas of ODSBR are:

a) broadcasting authenticated route requests and route replies;

b) attack detection by comparing the number of packet losses with a pre-defined threshold;

c) adaptive probing mode, specified by a source;

d) authenticated acknowledgements for locating a misbehaving link on the path by using binary search;

e) path selection metric with security in mind;

f) link weight management.

ODSBR detects Byzantine link after log n faults have occurred (n – length of a routing path), avoids this link and bounds the effect which may be caused by an adversary. Wireless-specific attacks are classified, investigated their harmful effect, and they are arranged according to the strength.

We identified the weak points of ODSBR:

A.) ODSBR adaptive acknowledgement probing mode is not time-optimal, and especially it is **very time-inefficient** in the face of colluding Byzantine adversaries which use strategic positioning. For example, ODSBR needs a lot of faults and time to locate a path segment of colluding Byzantine adversaries, which **overlaps** at least two binary probing intervals. It is very important, because if, for example, colluding adversaries approach a central strategic positioning, then such an attack would be the most harmful (according to the analysis in [11]).

Let us assume that three colluding Byzantine adversaries A1, A2, A3 form a segment of two adjacent misbehaving links on the routing path:

S - A1 - A2 - A3 - D

which consists of the compromised central (median) router A2 and the two of its also compromised neighbors from both sides (A1 and A3). Assume in the given network topology there exists (at least) one another correct path between source and destination. Assume that all the previous time the routers A1, A2, A3 behaved correctly.

As far as a decision to identify a link as faulty is made by the detection component of the protocol, then the source and the destination in the given moment don't know that routers A1, A2, A3 have been compromised. Therefore, it is possible, that according to the existing metrics the source and the destination will be continuing to choose the faulty path: S - A1 - A2 - A3 - D for routing the packets **during some amount of time**.

This situation will take place until the fault (the link A1 - A2) will be detected. After that the link weight management algorithm will increase the link counter. Then the traffic would be rerouted if there exists another path with the lower metrics.

Now, let's **time-measure** the detection process:

1st round: the source and destination can not validate traffic between themselves, and then during the next round, the source will add the node in the middle (A2) into the probe list.

2nd round: the source and that central node A2 will not validate the traffic between themselves.

3rd – log n-th rounds: this path sub-division process will continue until after log n faults the one detected failure will correspond to a faulty link, adjacent to the central node from the side, which is closer to the source (A1 - A2).

ODSBR after log n faults will have detected **only one of the two misbehaving link**. At the same time the given path at whole will still remain to be faulty (because of A2 – A3 will still remain to be not detected). Moreover, one of the two misbehaving links will be detected only at the **latest** round of the adaptive probing process. Therefore, the adaptive probing mode of **ODSBR allows the maximal possible detection time to the most harmful type of attack** (according to the ranking [11]).

B.) ODSBR addresses only one type of data forwarding misbehavior: packet dropping.

C.) The threshold value for distinguishing between 'normal' and 'anomaly' packet loss rates is fixed and constantly determined by the source. It is not an optimal solution because it doesn't consider possible dynamical changes of factors affecting 'normal' packet loss in the network. The problem is that the given threshold value determines the amount of packet loss that an adversary is allowed to create without being detected.

2.2. Watchdog

The approach proposed in [12] is aimed to identify misbehaving routers in ad-hoc networks. It is based on promiscuous overhearing of neighboring nodes, which

forwarding packets to other destinations. If a node does not overhear a neighbor forwarding more than a threshold number of packets, it concludes that the neighbor is adversarial.

The main limitations of Watchdog are: a) it cannot work when power control or multi-rate are used; b) it cannot detect colluding adversaries.

2.3. Forwarding misbehavior in ad-hoc networks

Detection and accusation mechanism for data forwarding misbehavior in ad-hoc networks presented in [13]. It uses Conversation of Flow principle, that all packets sent to a node, and not destined for that node, are expected to exit the node. But the design is different from WATCHERS.

Gonzales et all take into consideration mobility and broadband nature of wireless medium. According to their approach each node is required to keep three tables: an overheard nodes table, a detection table, and an accusation table.

The overheard nodes table contains the IDs of those nodes that have been overheard recently through promiscuous listening. The detection table contains the IDs of those nodes that have been detected as misbehaving and the number of times their misbehavior has been reported.

The accusation table keeps the IDs of those nodes that have been accused of misbehavior. Nodes are accused of misbehavior because they have reached within a predefined period of time the number of misbehavior detections required to be accused.

However, using of fixed thresholds, reliance on promiscuous listening (overhearing), and addressing only packet loss cause to several practical limitations of this detection mechanism.

2.4. Detecting disruptive routers in sensor networks

The paper [14] presents a lightweight hint-based approach for detecting disruptive routers in wireless sensor networks. The main idea is that the source and every intermediate node should probabilistically send a hint (digest) of the packet to the destination.

The hint is used by the destination to verify whether the corresponding packet reaches its destination and to verify its integrity. The hint also contains a set of nodes that should not be used for routing the given hint. Based on the packets and the hints received, the base station detects and locates disruptive routers.

Disadvantages of the given approach are:

a) it could work only when there is at most one disruptive router in the network;

b) it doesn't address selective packet dropping depending on destination or payload.

2.5. The two-hop ACK scheme

The 2ACK scheme presented in [15] is based on sending two-hop acknowledgment packets in the opposite direction of the routing path. Only a fraction of the received data packets are acknowledged to reduce routing overhead. The 2ACK scheme implemented on top of destination source routing.

The problem here is that 2ACK in order to be inplemented needs some parameters to be set and specific information to be available for the sender and the observing node. But it is not easy to realize.

Conclusion

There are a lot of designing complexities and limitations of routing protocols which must be robust to strategic Byzantine attacks on data forwarding plane. Today every routing protocol might be attacked effectively.

The reason is in weaknesses of security mechanisms and mistakes made by protocol designers. Currently protocols are mostly designed and specified in the form of unstructured prosaic (textual) descriptions with very little formalism.

The only solution is to make protocol designing approach more mature by means of formal methods. Further research direction is using Colored Petri nets and UML for specifying and verifying of data forwarding plane of routing protocols.

References

1. Barbir A. Generic Threats to Routing Protocols / A. Barbir, S. Murphy, Y. Yang // RFC 4593. – 2006.

2. Mizrak A.T. Detecting and Isolating Malicious Routers / A. Mizrak, Y. Cheng, Marzullo, K. Savage // IEEE Transactions on Dependable and Secure Computing. – 2006. – Vol. 3 (3) – P. 230-244.

3. Perlman R. Network Layer Protocols with Byzantine Robustness / R. Perlman // Ph.D. thesis, MIT. – 1988.

4. Perlman R. Routing with byzantine robustness / R. Perlman // Tech. Rep. TR-2005-146, Sun Microsystems. – 2005.

5. Lamport L. The byzantine generals problem / L. Lamport, R. Shostak, M. Pease // ACM Trans. Program. Lang. Syst.– 1982. – P. 382–401.

6. Cheung S. Protecting Routing Infrastructures from Denial of Service Using Cooperative Intrusion

Detection / S. Cheung, K. Levitt // Proc. New Security Paradigms Workshop, 1997.

7. Bradley K.A. Detecting Disruptive Routers: A Distributed Network Monitoring Approach / K.A. Bradley, S. Cheung, N. Puketza, B. Mukherjee, R.A. Olsson // Proc. IEEE Symp. Security and Privacy, 1998. – P. 115-124.

8. Hughes J.R. Using Conservation of Flow as a Security Mechanism in Network Protocols / J.R. Hughes, T. Aura, M. Bishop // Proc. IEEE Symp. Security and Privacy, 2000. – P. 132-131.

9. Herzberg A. Early detection of message forwarding faults / A. Herzberg, S. Kutten // SIAM J. Comput. – 2000. – Vol. 30(4). – P. 1169–1196.

10. Avramopoulos I. Highly secure and efficient routing / I. Avramopoulos, H. Kobayashi, R. Wang, A. Krishnamurthy // In Proceedings of INFOCOM Conference, March 2004.

11. Awerbuch B. ODSBR: An On-Demand Secure Byzantine Resilient Routing Protocol for Wireless Ad Hoc Networks / B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, H. Rubens // ACM Transactions on Information Systems Security (TISSEC), 2007.

13. Marti S. Mitigating routing misbehavior in mobile ad hoc networks / S. Marti, T. Giuli, K. Lai, M. Baker // In Proceedings of ACM Annual International Conference of Mobile Computing (MOBICOM), 2000.

14. Gonzalez O.F. Detection and Accusation of Packet Forwarding Misbehavior in Mobile Ad-Hoc Networks / O. F. Gonzalez, G. Ansa, M. Howarth, G. Pavlou // Journal of Internet Engineering. – 2008. – Vol. 2 (1). – P. 17-23.

15. Cheung S. Detecting Disruptive Routers in Wireless Sensor Networks / S. Cheung, B. Dutertre, U. Lindqvist //, LNCS 4104, 2006. – P. 19–31.

16. Liu K. Acknowledgment-Based Approach for Detection of Routing Misbehavior in MANET / K. Liu, J. Deng, P.K. Varshney, K. Balakrishnan // IEEE Transactions on Mobile Computing. – 2007. – Vol. 6 (5). – P. 488 – 502.

Поступила в редакцию 15.02.2009

Рецензент: д-р техн. наук, проф. В.А. Заславский, Национальный университет им. Тараса Шевченко, Киев, Украина.

СТРАТЕГИЧЕСКИЕ АТАКИ НА ПЛОСКОСТИ ФОРВАРДИНГА ДАННЫХ В ПРОТОКОЛАХ МАРШРУТИЗАЦИИ С РОБАСТНОСТЬЮ К ВИЗАНТИЙСКИМ ОШИБКАМ

С.В. Гладыш

Статья посвящена проблеме робастности протоколов маршрутизации к «Византийским ошибкам». В центре внимания – слабости (уязвимости) протоколов маршрутизатии в плоскости форвардинга данных, а также стратегические «Византийские атаки». Проведен анализ и показаны ограничения нескольких протоколов маршрутизации. Обнаружены критические ошибки в протоколах и предложены эффективные сценарии атак. Подвергается критике существующая методология разаработки протоколов.

Ключевые слова: Византийские ошибки, форвардинг данных, робастность к ошибкам, обнаружение вторжений, протоколы маршрутизации

СТРАТЕГІЧНІ АТАКИ НА ПЛОЩИНІ ФОРВАРДИНГУ ДАНИХ В ПРОТОКОЛАХ МАРШРУТИЗАЦІЇ З РОБАСТНІСТЮ ДО ВІЗАНТІЙСЬКИХ ПОМИЛОК

С.В. Гладиш

Статтю присвячено проблемі робастності протоколів маршрутизації до «Візантійських помилок». В центрі уваги – слабкості (вразливості) протоколів маршрутизації в площині форвардингу даних, а також стратегічні «Візантійські атаки». Проведено аналіз та показано обмеження декількох протоколів маршрутизації. Виявлено критичні помилки в протоколах та запропоновано ефективні сценарії атак. Підвергнуто критиці існуючу методологію розробки протоколів.

Ключові слова: Візантійські помилки, форвардинг даних, робастність до помилок, виявлення вторгнень, протоколи маршрутизації

Гладыш Сергей Викторович – PhD-студент, исследователь-ассистент Департамента телематики Норвежского университета науки и технологии, Тронхейм, Норвегия, e-mail: sgladex@gmail.com.