Research Paper

Volume : 5 | Issue : 5 | May 2016 • ISSN No 2277 - 8179 | IF : 3.508 | IC Value : 69.48

Survey on Security of Channel Aware Protocols

Engineering

KEYWORDS : Channel aware protocol, security, opportunistic scheduler, cooperative relaying, routing in wireless networks

Himani K. Paronigar Student,Sarvajanik College of Engineering and Technology. Surat,India

Dr.Pariza Kamboj Professor,Sarvajanik College of Engineering and Technology, Surat,India

ABSTRACT

Third generation (3G) wireless cellular network exploit time-varying and location-dependent channel condition of each mobile users. The protocol using channel condition as one of its input parameter is called 'channel aware'. In channel aware protocol, user reports its current channel condition to the base station or resource allocator or source node and they uses these reports for assigning resources to the mobile users. In channel aware protocol, security aspects are very important. The vulnerability of these protocols lies on trusting the reports sent by mobile users. This can be distinguished as false channel condition reporting attack which is imposed by reporting false channel condition feedback. In this paper, we review the security aspects of all channel aware protocols.

Introduction

In wireless network, many protocols which uses channel condition as a parameter is called 'channel aware protocol'. Some of the channel aware protocol includes co-operative replaying, ad hoc routing protocol and opportunistic schedulers. These protocols utilize link's channel condition in different ways. Co-operative replaying uses link's condition for deciding appropriate alternative relay path for node with the poor channel condition .ad hoc network routing protocols can use channel condition as a routing metric[1] .while opportunistic schedulers uses link's channel condition for efficient resource utilization. The main goal of channel aware protocol is to use channel's condition to enhance network throughput. Security aspects of channel aware protocol are very crucial. There are several studies on its security aspects. Major drawbacks in security of channel aware protocol is that base station trust the report given by the users. Each user reports its channel condition to the base station/scheduler. In this scenario, user can falsely report its channel condition. There are two ways of reporting false channel condition: underclaiming and overclaiming[2]. Underclaiming means reporting its channel condition lower than actual condition. Overclaiming means reporting its channel condition better than actual condition. The effects of these underclaiming and overclaming of channel reports are different on different channel aware protocols. We will study these effects in later sections. Many authors have studied the security aspects of channel aware protocol and define strategies to overcome those security threats.

The rest of paper is organized as follow. In section 2, we summarize the security aspects of opportunistic schedulers. In section 3, we summarize the security aspects of cooperative relaying. In section 4, we summarize the security aspects of ad hoc network routing protocol. Section 5 concludes the paper.

security aspects in opportunisitc schedulers

Opportunistic scheduler is a resource scheduler that utilizes channel condition of each user for efficient resource management. It assigns resources to the user which is having best channel condition at a particular time. In order to get more time slots, attacker can overclaim its channel condition.Underclaiming its channel condition is not beneficial to user. Here are some work in which security aspects of channel aware opportunistic scheduler is studied:

1. Exploiting and defending opportunistic scheduling in cellular network: [3]

The main focus of this paper is to study of security of Proportional Fair (PF) and Temporal Fair (TF) opportunistic scheduler. They have discovered two vulnerabilities:

1) Both schedulers trust the channel condition report submitted by the mobile user.

2) They provide fairness guarantees within the single cell.

First vulnerability is caused by a malicious mobile device reporting fake channel condition and second vulnerability is caused by initiating unnecessary handoff to bypass per-cell fairness guarantee. They have proposed two defense mechanism to avoid above mentioned second vulnerability. First, they propose to expand the PF and TF schedulers with priority queue and round robin to mitigate the attack. Unnecessary handoff of malicious users increases the average interpacket transmission delay. It will create bad impact on delay-sensitive applications, such as Voice over IP (VoIP). To avoid this problem, base stations can use priority queues. In particular, base station gives high priority to the traffic with the delay constraint, such as VoIP traffic, while scheduling other traffic, such as web browsing, with low priority. To provide fairness amongst all users, round-robin scheduler can be combined with any other scheduler so that each user roughly got the same number of time slots over long period of time. Second, they propose a robust handoff procedure to ensure that only honest users can do handoff while preventing attackers from stealing bandwidth. When mobile devices hands off, the new base station does not receive the device's average data rate from its previous base station, but assign a small or average value as the device's initial average rate. In their robust handoff scheme, they have derived the equation for calculating initial value of throughput. When user moves from cell A to cell B, the base stations covering these two cells can decide an initial average throughput value for user in cell B. Let N_A and N_B be the number of users in cells A and B, respectively. Let R_A be the current average rate of the user before handoff. The initial value after handoff, R^{init}_B , is set as

$$R_B^{init} = \frac{R_A(i)}{\frac{\log(N_A)}{N_A}} \frac{\log(N_B)}{N_B} \cdot \left(1 - \frac{1}{t_c}\right) \qquad (1)$$

2. On the Vulnerability of the Proportional Fairness Scheduler to Retransmission Attacks: [4]

Proportional Fairness Scheduler (PFS) is largely studied in a model, where frame loss does not occur. But that is not a case with practical scenarios. When it is being studied in frame loss environment, it is vulnerable to an attack, that is-retransmission attack. Suppose at time t, scheduler transmits to user U_i. Now at time t+1, suppose U_i tells scheduler that frame is did not arrive properly. If frame loss is due to network fault,then it is fair to schedule U_i at time t+1.But what if U_i is malicious and announced fake NACK ? Then it is called "retransmission attack". To make PFS handle frame loss, they describe two treatment approaches- PFS with Slow Retransmission (PFS-SR) and PFS Fast Retransmission (PFS-FR). In PFS-SR ,the frame will be retransmitted to the user only in the time slot when user obtain high-

est priority while in PFS-FR ,the frame will be transmitted to the user in the immediate next time slot.PFS assigns priority values to all users according to given equation,

$$V_i(t) = R_i(t)/A_i(t) \qquad (2)$$

Where $R_i(t)$ is the bit rate at which system send data to user U_i and $A_i(t)$ is the average throughput of Ui measured until time slot t. It is called Admitted Average in the Loss model, denoted by,

$$A_i(t+1) = (1- \varepsilon)A_i(t) + \varepsilon R_i(t)1_i^{rcv}(t) \qquad (3)$$

Where $1_i^{rcv}(t)$ =1 only if the user confirms the receipt of frame

by sending ACK. It means that if user have received frame successfully, then it is harder for him to get next time slot. PFS-SR and PFS-FR both are vulnerable to retransmission attack if Admitted Average method is used. So they have proposed two new averaging method-transmission average and effective average. The aim behind this solution is to pay all the users with the efforts the system invests in them instead of charging them with what they admit they got. This way, the ACK/NACK feedbacks of the users cannot influence the scheduling decisions. In transmission average scheme $A_i(t)$ is updated using following equation:

$$A_i(t+1)= R_i(t)1^{snd}{}_i(t) \qquad (4)$$

Where $R_i(t)$ is bit rate at which system send data to user U_i and $1^{snd}{}_i(t)$=1 if scheduler send frame to U_i regardless of NACK/ACK feedback. But transmission average method does not provide fairness. So to overcome this flaw they have proposed effective average method. In this scheme $A_i(t)$ is updated using following equation:

$$A_i(t+1)= R_i^e(t)1^{snd}{}_i(t) \qquad (5)$$

Where $1^{snd}{}_i(t)$ is calculated in the same way as in transmission range and $R_i^e(t)$ is effective rate ,calculated as $G_i(t)R_i(t)$ where $G_i(t)$ is the probability of successful transmission when sending data in rate $R_i(t)$ given the SNR value he reported for that time slot. These both scheme work well with both PFS-FR and PFS-SR.

3. Trustworthy Operations in Cellular Networks: The Case of Proportional Fairness Scheduler [5]:

Scheduling decision of proportional fairness is based on the channel quality metrics and Automatic Repeat reQuest (ARQ) feedback reports provided by the User's Equipment (UE). So the malicious UE can exploit the trust by faking their reports. They have proposed trust worthy version of PF schedulers TPF, to reduce the effect of Denial-of-service attack (DoS). Based on the channel condition reports by the user, they assign the probability to possible ARQ feedbacks. This probability associated with the actual ARQ report is used to assess the UE's reporting trustworthiness. They have adapted the scheduling mechanism to give higher priority to more trusted users.

security aspects in cooperative relaying

In Cooperative relaying network architectures, a node that has poor channel condition route its packet through a node with a good channel condition in order to improve system throughput. To find appropriate relay path, cooperative relay protocol distribute channel condition information of each user. The route with the best channel condition is to be chosen. Now when node under claims its channel condition, it is less likely to be chosen. But if an attacker overclaims its channel condition it is more likely to be chosen. As a result, overclaiming channel condition degrades the performance of protocol.

1. UCAN: A Unified Cellular and Ad-Hoc Network Architecture [6]:

In UCAN, they have proposed novel greedy and on-demand protocols for proxy discovery and ad-hoc routing to improve reliability. Mobile client experiencing high downlink channel rate receives route request and sends a proxy application message to base station. They have devised two proxy discovery protocols: Greedy and on-demand. Further, they have propose a secure crediting mechanism to inspire users to take part in relaying packets for others.Both,intermediate clients and proxy are awarded with the credits. They have identified two problems: One is the deletion of legitimate clients and the other is addition of extra clients. They have solved this two problems by piggybacking a single keyed Message Authentication Code(MAC) in the route request message.MAC authenticates the intermediate clients and proxy so that the base station can provide credit to only real relayers.

2. Secure Unified Cellular Ad Hoc Network Routing [7]:

SUCAN, routing protocol secures against both selfish and malicious attackers. They used incentives and penalties to eliminate the hosts that want to take performance advantages. Incentives are given for correct participation. Incentives can be in different forms based on what is advantageous for an individual mobile node. Secondly, they use grudging. Grudging is remembering previous unsuccessful encounters, Grudging is remembering previous unsuccessful encounters, so that if a node holds a grudge against another node, the former will no longer interact with the latter. Moreover, SUCAN also provides limited level of data integrity and confidentiality.

3. JANUS: A Framework for Scalable and Secure Routing in Hybrid Wireless Networks [8]:

JANUS, a framework that provides scalable, secure, and efficient routing for hybrid wireless networks. It consists of four components: an efficient routing algorithm, a crediting protocol providing protection against selfish nodes, and two security components providing protection against malicious nodes. The first security component protects the path reservation and control messages, while the second efficiently detect and isolate attacks against data forwarding. Routing algorithm, DST, Selects path with is having highest throughput for each user from base station. DST achieves this by using a dynamic spanning tree of the network, rooted at the base station. They have considered attacks, those are freeloading caused by selfish attackers and selective data forwarding caused by malicious attackers, which targets the data forwarding service and rate inflation, tunneling, ghost requests, and path scrambling, which affect the routing protocol.

IV. SECURITY IN ROUTING PROTOCOL IN WIRELESS NETWORKS

Routing protocol is wireless ad hoc networks discovers path between nodes. There is multiple paths available between source and destination. Routing protocol needs to choose among valid paths. Routing metrics is the value associated with the path that represents its desirability of being chosen. One of the possible routing metrics is channel condition of each link in the path. An intermediate node in the path can overclaim its channel condition in order to increase the probability of being chosen. If intermediate node underclaim it, then source node do not choose a route through that intermediate node. So overclaiming can adversely affect performance of routing.

1. Channel-Aware Routing in MANETs with Route Handoff (CA-AOMDV) [9]:

Channel-aware AOMDV is an enhanced, channel-aware version of the AOMDV [10] routing protocol. The key aspect of this enhancement is that it uses channel quality information as path availability. This approach allows reuse of paths which becomes

Volume : 5 | Issue : 5 | May 2016 • ISSN No 2277 - 8179 | IF : 3.508 | IC Value : 69.48

unavailable due to its low channel condition, rather than simply discarding it. They have used the channel average non-fading duration (ANFD) as a measure of link stability, combined with the traditional hop-count measure for path selection. The average fading duration (AFD) is used to determine when to bring a path back into play, which is previously marked as unavailable. The overall effect is a protocol with improved routing decisions leading to a more robust network.

V.CONCLUSION AND FUTURE SCOPE

In this paper, we have studied security aspects of three channel aware protocols. it is clear that trusting the channel condition report submitted by the mobile user can cause an attack and hence reduce the performance of other users. Rather than trusting user's channel condition reported by users, there is a need to develop a secure channel condition estimation scheme to prevent overclaiming attack.

References

1. Y.-C. Hu and A. Perrig, "A survey of secure wireless ad hoc routing," IEEE Security Privacy, vol. 2, no. 3, pp. 28–39, May/Jun.2004.
2. Kim, Dongho, and Yih-Chun Hu. "A study on false channel condition reporting attacks in wireless networks." Mobile Computing, IEEE Transactions on 13.5 (2014): 935-947.
3. R. Racic, D. Ma, H. Chen, and X. Liu, "Exploiting and defending opportunistic scheduling in cellular data networks," IEEE Trans. Mobile Comput., vol. 9, no. 5, pp. 609–620, May 2010.
4. U. Ben-Porat, A. Bremler-Barr, H. Levy, and B. Plattner, "On the vulnerability of the proportional fairness scheduler to retransmission attacks," in Proc. IEEE INFOCOM, Shanghai, China, Apr.2011, pp. 1431– 1439.
5. Pelechrinis, K.; Krishanmurthy, P.; Gkantsidis, C., "Trustworthy Operations in Cellular Networks: The Case of PF Scheduler," in Parallel and Distributed Systems, IEEE Transactions on , vol.25, no.2, pp.292-300, Feb. 2014
6. H. Luo, R. Ramjee, P. Sinha, L. E. Li, and S. Lu, "Ucan: A unified cellular and ad-hoc network architecture," in Proc. ACM MobiCom, San Diego, CA, USA, 2003, pp. 353–367.
7. Haas, J.J.; Yih-Chun Hu, "Secure Unified Cellular Ad Hoc Network Routing," in Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE , vol., no., pp.1-8, Nov. 30 2009-Dec. 4 2009
8. Nita-Rotaru, C.; Carbunar, B.; Nita-Rotaru, C., "JANUS: A Framework for Scalable and Secure Routing in Hybrid Wireless Networks," in Dependable and Secure Computing, IEEE Transactions on , vol.6, no.4, pp.295-308, Oct.-Dec. 2009
9. Xiaoqin Chen; Jones, Haley M.; Jayalath, D., "Channel-Aware Routing in MANETs with Route Handoff," in Mobile Computing, IEEE Transactions on , vol.10, no.1, pp.108-121, Jan. 2011
10. M.K. Marina and S.R. Das, "On-Demand Multipath Distance Vector Routing in Ad Hoc Networks," Proc. Ninth Int'l Conf. Network Protocols (ICNP), pp. 14-23, Nov. 2001.