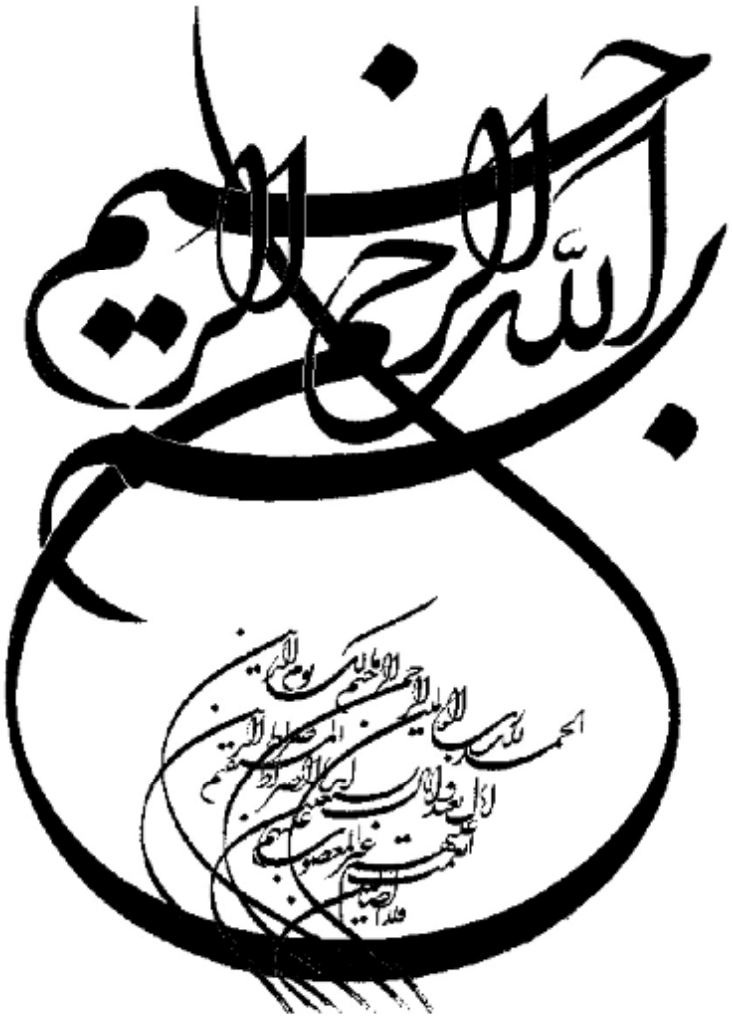
بسم الله الرحمن الرحیم

دانشگاه صنعتی اصفهان

دانشکده برق و کامپیوتر

گمنام‌سازی پروتکل‌های مسیریابی در شبکه‌های اقتضایی سیار به منظور مقابله با حملات تحلیل ترافیک

پایان‌نامه کارشناسی ارشد مهندسی برق- مخابرات

الهه شکل‌آبادی

استاد راهنما

دکتر مهدی برنجکوب

۱۳۹۰

دانشگاه صنعتی اصفهان

دانشکده برق و کامپیوتر

پایان‌نامه‌ی کارشناسی ارشد رشته‌ی مهندسی برق – مخابرات خانم الهه شکل‌آبادی

تحت عنوان

گمنام‌سازی پروتکل‌های مسیریابی در شبکه‌های اقتضایی سیار به منظور مقابله با حملات تحلیل ترافیک

در تاریخ ۹۰/۱/۲۲ توسط کمیته‌ی تخصصی زیر مورد بررسی و تصویب نهایی قرار گرفت.

۱- استاد راهنمای پایان‌نامه	دکتر مهدی برنجکوب
۲- استاد مشاور پایان‌نامه	دکتر حسن سعیدی
۳- استاد داور	دکتر محمد دخیل‌علیان
۴- استاد داور	دکتر پژمان خدیوی
سرپرست تحصیلات تکمیلی دانشکده	دکتر سید محمود مدرس هاشمی

تشکر و قدردانی

حمد، سپاس و ستایش بی حد خدای متعال را که بنده را مرهون اقیانوس بی پایان و بی کران الطاف خود قرار داد. مرا برای اعتلای قدمی که پیمودم همراهی نمود و شد و دیگر اتکا به او، دانش را در برابر من گشود و با همه وجود با خضوع و خشوع، خداوند منان را سپاسگزارم به خاطر آنچه به لطف و رحمت حقیقی به من ارزانی داشته و هر آنچه به حکمت خویش از من دریغ نموده است.

اکنون که توانسته‌ام به یاری ذات پاک حق تعالی این مقطع کوتاه از تحصیلاتم را پشت سر گذاشته و قدمی دیگر در راستای اعتلای خود و جامعه‌ام بردارم بر خود واجب دانستم مراتب تشکر و قدردانی خود را از تمام کسانی که در این مرحله یار و مشوق من بوده‌اند، اعلام دارم.

پیش از هر کس لازم می‌دانم از اعضای صبور و پرمهر خانواده‌ام و به ویژه از پدر و مادر عزیز و گرامی‌ام که نه تنها در تمام مراحل زندگی یار، همراه، پشتیبان، مشوق و همدم بوده‌اند، خاضعانه و خاشعانه تشکر و سپاسگزاری نمایم.

در طی مراحل تحقیق و تدوین این پایان‌نامه از کمک و راهنمایی‌های استادان ارجمند و بزرگواری برخوردار بوده‌ام که لازم است مراتب قدردانی و تشکر خالصانه خود را نسبت به آنان ابراز دارم. از آقای دکتر مهدی نیک‌کوب، استاد راهنمای پایان‌نامه که در طی این مدت نظرات سودمندشان راهگشا بود، کمال تشکر و تقدیر را دارم. بی‌شک بدون راهنمایی‌های ارزنده و پیگیری‌های مداوم ایشان، انجام این پایان‌نامه میسر نبود. امید آن دارم که شایسته زحمات ایشان بوده باشم و روزی بتوانم به نحو شایسته‌ای جبران گوشه‌ای از محبت‌های بی‌دریغشان را بنمایم. از آقای دکتر حسین سعیدی استاد مشاور پایان‌نامه که در تدوین هر چه بهتر این پایان‌نامه از راهنمایی‌های ارزشمندشان استفاده کرده‌ام، سپاسگزاری و قدردانی می‌نمایم. همچنین از آقایان دکتر محمد خلیل علایی و دکتر پژمان خدیوی که زحمت داوری این پایان‌نامه را متقبل شدند و با حضور در جلسه دفاع از پایان‌نامه نکات مفیدی را یادآور شدند، تشکر می‌کنم.

دوستان عزیز و بزرگوارم که دوران تحصیل در این دانشگاه را به دوره‌ای سرشار از نشاط، شادابی و خاطرات زیبا مبدل نمودند، صمیمانه تشکر می‌کنم. سربلندی، شادکامی، پیروزی و موفقیت روزافزون این عزیزان، آرزوی همیشگی من است.

لیلا سگال آبادی، دانشگاه صنعتی اصفهان، فروردین ماه ۱۳۹۰

کلیه‌ی حقوق مادی مترتب بر نتایج مطالعات، ابتکارات و نوآوری‌های ناشی از تحقیق موضوع این پایان‌نامه (رساله) متعلق به دانشگاه صنعتی اصفهان است.

تقدیم به آنان که وجودم هدیه وجودشان است:

پدر و مادر عزیز و مهربانم،

آموزگارانی که برایم زندگی، بودن و انسان بودن را معنا کردند...

فهرست مطالب

عنوان **صفحه**

فهرست شکل‌ها

عنوان **صفحه**

چکیده

در دهه‌ی اخیر، تحقیقات در زمینه حفظ حریم خصوصی در شبکه‌های MANET افزایش یافته است. نقض حریم خصوصی به منظور دستیابی به اطلاعات شخصی شبکه و اعضای آن هدف اصلی مهاجم در حمله تحلیل ترافیک می‌باشد. در واقع در حمله تحلیل ترافیک دشمن سعی دارد با مشاهده و بررسی الگوی ترافیک شبکه و تغییرات آن به اطلاعات ارزشمندی در مورد مشخصه‌های ترافیک ارسالی مثل هویت طرفین ارتباط، فرکانس ارسال داده، هویت گره‌های روی مسیر، مکان و الگوی حرکت یک گره وغیره دست یابد. نشت چنین اطلاعاتی، بسیاری از سناریوهایی که از نظر امنیتی حساس می‌باشند را در معرض خطر قرار می‌دهد. از سوی دیگر، با در نظر گرفتن کاربردهای خاص MANET، که به طور عمده در محیط‌های نظامی، شبکه‌های موقت کنفرانس‌ها و عملیات امداد و نجات به کار گرفته می‌شود، حفظ حریم خصوصی در این شبکه‌ها از اهمیت بالایی برخوردار است. یکی از شیوه‌های مؤثر برای مقابله با حملات تحلیل ترافیک، پنهان نگه داشتن اطلاعات مسیریابی از دید مهاجم و حتی گره‌های مجاز شبکه است. تاکنون به منظور تأمین امنیت مسیریابی در MANET، پروتکل‌های مسیریابی امن متعددی پیشنهاد شده‌اند اما یک پروتکل مسیریابی امن ذاتاً قادر به مقابله با حملات تحلیل ترافیک نمی‌باشد. بنابراین علی‌رغم وجود پروتکل مسیریابی امن برای MANET، ارائه‌ی سرویس گمنامی توسط پروتکل مسیریابی در راستای مقابله با حملات تحلیل ترافیک به منظور پنهان نمودن اطلاعاتی مثل هویت گره‌های شبکه و توپولوژی شبکه الزامی است. هدف از این پایان‌نامه دسترسی به الگوریتمی بهبودیافته جهت مقابله با حملات تحلیل ترافیک می‌باشد. برای این منظور ابتدا حملات تحلیل ترافیک و شیوه‌های مقابله با آن‌ها در MANET مورد بررسی قرار گرفته و دسته‌بندی شده‌اند. سپس به طور خاص، پروتکل‌های مسیریابی گمنام به عنوان یکی از روش‌های مؤثر برای مقابله با حملات تحلیل ترافیک مورد مطالعه و ارزیابی قرار گرفته‌اند. در این راستا تعدادی از پروتکل‌های مسیریابی گمنام موجود برای MANET بررسی شده‌اند. نتایج حاصل از مطالعه و بررسی این پروتکل‌ها، امکان گمنام‌سازی پروتکل‌های مسیریابی موجود را آشکار نمود. به منظور دستیابی به پروتکل مسیریابی گمنام مطلوب، پروتکل مسیریابی پایه‌ی AODV و پروتکل مسیریابی ARAN ،که از یکی از شناخته‌شده‌ترین پروتکل‌های مسیریابی امن در MANET می‌باشد، در این پایان نامه مورد توجه قرار گرفته است. پروتکل AnonAODV به عنوان نسخه‌ی گمنام پروتکل AODV در راستای بهبود پروتکل گمنام PseudoAODV ارائه شده است. این پروتکل امکان ارائه‌ی سرویس‌های گمنامی در حضور مهاجمین غیرفعال سراسری را فراهم می‌آورد. پروتکل AnonAODV صرفاً بر روی گمنام سازی AODV متمرکز شده است، در حالی که گمنام‌سازی پروتکل ARAN، منجر به دستیابی به یک پروتکل مسیریابی امن گمنام تحت عنوان AARAN شده است. حفظ ویژگی‌های امنیتی پروتکل ARAN در کنار دستیابی به سرویس‌های گمنامی، خط مشی طراحی این پروتکل در نظر گرفته شده است.

کلمات کلیدی: ۱- شبکه‌های اقتضایی سیار ۲- حمله تحلیل ترافیک ۳- گمنامی ۴- حریم خصوصی ۵- مسیریابی گمنام

مراجع

[1] Shannon, C.E., "Communication Theory of Secrecy Systems," *Bell Systems Technical Journal*, Vol. 28, pp. 656-715, 1949.

[2] Çayırcı, E. and Rong, Ch., "Security in Wireless Ad Hoc and Sensor Networks," *John Wiley & Sons*, p. 109, 2009.

[3] Zhang,Y., Liu, W. and Lou,.W., "Anonymous Communications in Mobile Ad Hoc Networks," *International Conferences of the IEEE Computer and Communications Societies*, vol. 3, pp. 1940-1951, 2005.

[4] Shokri, R., Yabandeh, M. and Yazdani, N., "Anonymous Routing in MANET Using Random Identifiers," *Proceedings of the Sixth International Conference on Networking* (*ICN'07*), p. 2, 2007.

[5] Kong, J. and Hong, X., "ANODR: Anonymous on demand routing with untraceable routes for MANETs," *ACM MobiHoc*, 2003.

[6] Bo, Z., Zhiguo, W., Kankanhalli, M.S., Feng, B. and Deng, R.H., "Anonymous secure routing in mobile ad-hoc networks," *29th of Annual IEEE International Conference on Local Computer Networks*, pp. 102-108, 2004.

[7] Seys, S. and Preneel, B., "ARM: Anonymous routing protocol for mobilead hoc networks," *Proceedings of*. 20th *International Conference on Advanced Information Networking and Applications, AINA*, pp. 133–137, Apr. 2006.

[8] Fusenig, V., Spiewak, D. and Engel, T., "Acimn: A protocol for Anonymous Communication In Multi hop wireless networks," *Proceeding of the. Sixth Australasian Information Security Conference*, 2008.

[9] Qiaolin, H., Qingyuan, H., Biao, H., Baokang, Z. and Su, J., "MSR: A Novel MPLS-Like Secure Routing Protocol for Mobile Ad Hoc Networks," *International Conference on Networks Security, Wireless Communications and Trusted Computing, NSWCTC '09*, pp. 129-132, 2009.

[10] Rahman, S.M., Nasser, N., Inomata, A., Okamoto, T., Mambo, M. and Okamoto, E., "Anonymous authentication and secure communication protocol for wireless mobile ad hoc networks," *Wiley InterScience, Security and Communication Networks*, vol. 1, no. 2, pp. 179–189, 2008.

[11] Díaz, C., Seys, S., Claessens, J. and Preneel, B., "Towards measuring anonymity," *Proceedings of the 2nd international conference on Privacy enhancing technologies, Springer-Verlag Berlin*, pp. 54-68, 2003.

[12] Dijiang, H., "On Measuring Anonymity For Wireless Mobile Ad-hoc Networks,", *Proceedings 31st IEEE Conference on Local Computer Networks*, pp. 779-786, 2006.

[13] Gaup-Moe , E., "Quantification of Anonymity for Mobile Ad Hoc Networks" *Electronic Notes in Theoretical Computer Science (ENTCS), Springer-Verlag*, Vol. 244, August, 2009.

[14] Perkins, Ch., E. , Belding-Royer, E. and Das, S., "Ad hoc On-Demand Distance Vector (AODV) Routing protocol," *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*,.pp. 90-100, 1999.

[15] Sanzgiri, K., LaFlamme, D., Dahill, B., Levine, B., Shields, C. and Belding-Royer, E., "Authenticated routing for ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 23, pp. 598-610, 2005.

[16] http://en.wikipedia.org/wiki/Traffic_analysis, last modified on November 2010.

[17] Xinwen, F., Graham, B., Bettati, R. and Wei, Z., "Active traffic analysis attacks and countermeasures," *Proceedings of the International Conference on Computer Networks and Mobile Computing*, ICCNMC 2003, pp. 31-39, 2003.

[18] Pfitzmann, A. and Hansen, M., "Anonymity, unlinkability, undetectability, unobservability, pseudonymity and identityManagement a consolidated proposal for terminology", Available at online http://dud.inf.tu-dresden.de/Anon Terminology.shtml, February 2008 (version 0.31).

[19] Kong, J., "Anonymous and Untraceable Communications in Mobile Wireless Networks", *PhD. dissertation, University of California*, 2004.

[20] Kong, J., Hong, X. and Gerla, M., "A new set of passive routing attacks in mobile ad hoc networks," *Proceedings of the IEEE Conference on Military Communications*, MILCOM 2003, pp. 796-801, 2003.

[21] Li, P., Lin, Y. and Zeng, W., "Search on Security in Sensor Networks," Journal of Software, vol. 17, pp. 2577-2588, 2006.

[22] Raymond, J., "Traffic analysis: Protocols, attacks, designissues and open problems," *Proceedings of International Workshop on Design Issues in Anonymity and Unobservability*, Springer-Verlag, pp. 10–29, 2001.

[23] Choi, H., McDaniel, P. and La, T.F., "Privacy Preserving Communication in MANETs," 4th Annual IEEE Communications Society Conference, San Diego, pp. 233-242, 2007.

[24] Levine, B.N., Wang, M.K. and Wright, M., "On timing attacks in low-latency mix-based systems," *Proceedings of the 8th International Conference on Financial Cryptography*, 2004.

[25] Adam, B., ller, U. and Anton, S., "Traffic Analysis Attacks and Trade-Offs in Anonymity Providing Systems," *Proceedings of the 4th International Workshop on Information Hiding: Springer-Verlag*, 2001.

[26] Cao, J., Stojmenovic, I., Jia, X., Das, S., Wu, X., Liu, J., Hong, X. and Bertino, E., "Achieving Anonymity in Mobile Ad Hoc Networks Using Fuzzy Position Information," *Proceedings of the 2nd International Conference in Mobile Ad-hoc and Sensor Networks, Springer Berlin/Heidelberg*, vol. 4325, pp. 461-472, 2006.

[27] Martin, D., Serjantov, A., Mathewson, N. and Dingledine, R., "Practical Traffic Analysis: Extending and Resisting Statistical Disclosure," *4th international workshop on Privacy Enhancing Technologies, Springer Berlin/Heidelberg*, vol. 3424, pp. 707, 2005.

[28] Durresi, A., Paruchuri,V., Durresi, M. and Barolli, L., "Anonymous Routing for Mobile Wireless Ad Hoc Networks," *International Journal of Distributed Sensor Networks*, vol. 3, no. 1, pp. 105-117, 2007.

[29] Jiejun, K., Xiaoyan, H., Sanadidi, M.Y and Gerla, M., "Mobility changes anonymity: mobile ad hoc networks need efficient anonymous routing," *Proceedings of 10th IEEE Symposium on Computers and Communications, ISCC 2005*, pp. 57-62, 2005.

[30] Berg, O., Berg, T., Haavik, S., Hjelmstad, J. and Skaug, R., "SpreadSpectrum in Mobile Communication" *Institution of Electrical Engineers, IEEE telecommunications series, London*,p. 458, 1998.

[31] Newman-Wolfe, R.E and Venkatraman, B.R, "High level prevention of traffic analysis" *In Seventh Annual ComputerSecurity and Applications Conference*, Dec. 1991.

[32] Wu, B., Wu, J., Fernandez, E.B., llyas, M. and Magliveras, S., "Secure and efficient key management in mobile ad hoc networks," *Journal of Network and Computer Applications*, vol. 30, pp. 937-954, 2007.

[33] Guan, Y., Li, C., Xuan, D., Bettati, R. and Zhao, W., "Preventing traffic analysis for real-time communication networks," *Proceedings of the military communications Conference, MilCom'99*, pp. 744-750, Oct. 1999.

[34] Shu, J., Vaidya, N.H. and Zhao, W., "Preventing traffic analysis in packet radio networks," *Proceedings in DARPA Information Survivability Conference & Exposition, DISCEX '01*, Vol.2, pp. 153-158, 2001.

[35] Lee, J. and Gerla., M., "Split Multipath Routing with Maximally Disjoint Paths in Ad Hoc Networks," *IEEE International Conference on Communications*, 2001.

[36] Marina, M.K. and Das, S.R., "AOMDV: Ad hoc On-demand Multipath Distance Vector Routing Protocol," *Proceedings of the 9th International Conference on Network Protocols*, pp. 14-23, 2001.

[37] Zhu, S., Setia, S. and Jajodia, S., "LEAP: Efficient Security Mechanisms for Large Scale Distributed Sensor Networks," *ACM Conference on Computer and Communications Security*, 2003.

[38] http://en.wikipedia.org/wiki/Padding_(cryptography), last modified on November 2010.

[39] Jiang, J., Vaidya, N. and Zhao, W., "Power-Aware Traffic Cover Mode to Prevent Traffic Analysis in Wireless Ad Hoc Networks," *In IEEE Infocom*, 2001.

[40] Chaum, D., "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–88, 1981.

[41] Jiang, J., Vaidya, N. and Zhao, W., "A Dynamic Mix Method for Wireless Ad Hoc Networks," *MILCOM*, Vol 2, pp. 873-877, 2001.

[42] Fu, X., "On Traffic Analysis Attacks and Countermeasures," *M.S. thesis, Communication Engineering Department, Texas A&M University*, 2005.

[43] Boneh, D. and Franklin, M., "Identity Based Encryption from the Weil Pairing", *SIAM Computing*, Vol. 32, No. 3, pp. 586-615, 2003.

[44] Berreto, L.M., Kim, H.Y. and Scott, M., "Efficient algorithms for pairing-based cryptosystems", *Advances in Cryptology - Crypto '2002, LNCS 2442*, pp.354-368, Springer-Verlag, 2002.

[45] Galbraith, S., Harrison, K. and Soldera, D., "Implementing the Tate Pairing", *Algorithm Number Theory Symposium - ANTS V, LNCS 2369, Springer-Verlag*, pp. 324-337, 2002.

[46] Molva, R., Tsudik, G., Westhoff, D., Ács, G., Buttyán, L. and Vajda, I., "Provable Security of On-Demand Distance Vector Routing in Wireless Ad Hoc Networks," *in Security and Privacy in Ad-hoc and Sensor Networks*, vol. 3813: Springer Berlin / Heidelberg, pp. 113-127, 2005.

[47] Gis, R. and Andreas, E., "Provably secure non-interactive key distribution based on pairings," Discrete Applied Mathematics, Coding and cryptography., vol. 154, pp. 270-276, 2006.

Defending against Traffic Analysis Attacks with the Use of Anonymous Routing Protocols

Elahe Sheklabadi
e.sheklabadi@ec.iut.ac.ir

Date of Submission: 2011/04/11

Department of Electrical and Computer Engineering

Isfahan University of Technology, Isfahan 84156-83111, Iran

Degree: M.Sc. Language: Persian

Supervisor: Mehdi Berenjkoub, brnjkb@cc.iut.ac.ir

Abstract

In recent decade, the topic of MANET privacy has been flourished. Privacy is the main aim of the traffic analysis attacks. Indeed, an adversary intercepts network traffic in order to infer sensitive information about network traffic characteristics such as the identities of communicating parties, location of nodes data transmission rate and motion pattern of nodes, in traffic analysis attacks. This may lead to severe threats in security-sensitive applications. In the other hand, privacy is considered as one of the most important security features in the specific applications of MANET including military networks and search and rescue operations. Concealing the routing information from adversary and even legitimate nodes is an effective method to resist against traffic analysis attack. Although the secure routing for MANETs has been extensively studied, traffic analysis attacks are still not well addressed. So, providing anonymous routing protocols i.e. routing protocols which include anonymity services is quite important. Using these protocols is necessary to resist against to traffic analysis attack in order to hiding some information such as the real identity of network nodes and network topology. The aim of this thesis is presenting an improved algorithm in order to defend against traffic analysis attacks. To this end, at the first, traffic analysis attacks and their countermeasures in MANET have been studied. These have been classified base on the adversary model, vulnerable security services and implementation layer. The comparison of countermeasure techniques showed that hiding routing information is highly effective to resist against traffic analysis attacks in MANET. In this thesis, the main concentration has been devoted to anonymous routing in MANETs. So, a number of anonymous routing protocols have been studied. Moreover, in this thesis, ARAN protocol, which has been known as one of the most secure routing in MANET, and AODV protocol have been considered in order to achieve an anonymous routing protocol. AnonAODV protocol, as an anonymous version of AODV protocol, has been proposed to improve a previous anonymous variant of it namely pseudoAODV protocol. This protocol provides anonymity services in the presence of global passive adversary. AnonAODV protocol has simply confused on providing anonymity in AODV protocol, while anonymous version of ARAN protocol results an anonymous secure routing protocol, namely AARAN. Both preserving security features of ARAN and achieving anonymity services have been considered as design policy of AARAN protocol. So, AARAN protocol is a secure routing protocol which also provides identity privacy, strong location privacy and route anonymity services.

Keywords:

Mobile Ad Hoc Network, Traffic Analysis Attack, Anonymity, Privacy, Anonymous Routing

Isfahan University of Technology

Department of Electrical and Computer Engineering

Defending against Traffic Analysis Attacks with the Use of Anonymous Routing Protocols

A Thesis

Submitted in partial fulfillment of the requirements

For the degree of Master of Science in Electrical Engineering - Communications

By

Elahe Sheklabadi

Evaluated and Approved by the Thesis Committee, On April 11, 2011

Mehdi Berenjkoub, Assistant Professor (Supervisor)

Hossein Saidi, Associate Professor (Advisor)

Mohammad Dakhilalian, Assistant Professor (Examiner)

Pejman Khadivi, Assistant Professor (Examiner)

Mahmoud Modarres Hashemi Associate Professor (Department Graduate Coordinator)

فصل اول
مقدمه

۱-۱ مقدمه

شبکه‌های اقتضایی سیار(MANET)[1] شبکه‌هایی هستند که بدون نیاز به زیرساخت ثابت و کنترل‌کننده‌ی مرکزی ایجاد می‌شوند. با توجه به محدودیت انتشار امواج رادیویی، ترمینال‌های موجود در این شبکه‌ها از طریق یک یا چند گام با هم در ارتباط هستند و لذا هر ترمینال قابلیت هدایت بسته‌های سایر ترمینال‌ها را داراست. این شبکه‌ها، شبکه-های بی‌سیم چند گامی[2] و شبکه‌های رادیویی بسته‌ای[3] نیز نامیده می‌شوند. در این شبکه‌ها، گره‌ها به خودی خود و عمدتاً با استفاده از الگوریتم‌های توزیع شده، عملیات کنترلی و شبکه‌ای موردنیاز برای برپایی و نگه‌داری شبکه را انجام می‌دهند.

هر چند این شبکه‌ها به علت عدم وابستگی به ساختار مشخص، توانایی پشتیبانی و پیاده‌سازی در بسیاری از کاربردها مثل ارتباطات بی‌سیم در عملیات نظامی، ماموریت‌های نجات و ماموریت‌های اکتشافی را دارند، اما به دلیل خصوصیات منحصر به فردشان، نسبت به شبکه‌های سیمی بیشتر در معرض آسیب‌های امنیتی می‌باشند. خصوصیاتی مانند استفاده از بستر ارتباطی بی‌سیم، حرکت گره‌ها و مشارکت اعضای شبکه در ارسال پیام باعث می‌شوند ترافیک شبکه، شامل اطلاعات گره‌های در حال ارتباط و داده‌های آن‌ها، بعضاً در اختیار گره‌های مهاجم قرار گیرد. این در

---

[1] Mobile Ad hoc NETworks
[2] Multihop wireless networks
[3] Packet radio networks

حالی است که کاربردهای خاص MANET مانند شبکه‌های ارتباطی نظامی، تجارت الکترونیکی و شبکه‌های موقتی برای کنفرانس‌ها، نیاز به پنهان ماندن مشخصه‌های ترافیک ارسالی را بیش از پیش می‌طلبند.

از نقطه نظر مهاجم، حمله‌ی تحلیل ترافیک، یکی از راه‌های مؤثر برای استخراج اطلاعات مفید و حساس در رابطه با ترافیک شبکه و به طور کلی نقض حریم خصوصی[1] به شمار می‌آید. در این حمله، دشمن از طریق مشاهده و بررسی ترافیک شبکه و تغییرات آن حتی بدون دستیابی به محتوای بسته‌ها می‌تواند به اطلاعات ارزشمندی درباره مشخصه‌های ترافیک در حال تبادل مثل هویت طرفین ارتباط، فرکانس ارسال داده، شناسایی گره‌های روی مسیر و الگوی پیام دست یابد. حمله‌ی تحلیل ترافیک به عنوان یکی از حملات امنیتی جدید و حل نشده در MANET به شمار می‌آید. در این حمله، نه تنها اطلاعات خصوصی شبکه و کاربران آن افشا می‌شود بلکه مهاجم پس از به دست آوردن این گونه اطلاعات می‌تواند نقاط استراتژیک و حساس شبکه را مورد حملات مؤثرتری مانند حملات منع سرویس قرار دهد و آسیب‌های جدی‌تری را به شبکه وارد نماید. بنابراین، بررسی حملات تحلیل ترافیک و طراحی و پیاده‌سازی پروتکل‌ها و مکانیزم‌هایی جهت مقابله با آن‌ها در MANET حائز اهمیت است.

از نقطه نظر مهاجم، ترافیک لایه‌ی شبکه و به طور دقیق‌تر پروتکل‌های مسیریابی، منبع خوبی برای دستیابی به اطلاعات خصوصی شبکه و کاربران آن به شمار می‌آیند. لذا طراحی مناسب این پروتکل‌ها به منظور ممانعت از نشت اطلاعات بسته‌های کنترلی مبادله شده در روند کشف مسیر از اهمیت زیادی برخوردار است.

تاکنون به منظور تأمین امنیت مسیریابی در MANET، پروتکل‌های مسیریابی امن متعددی معرفی شده‌اند. اما یک پروتکل مسیریابی امن ذاتاً قادر به مقابله با حملات تحلیل ترافیک نیست زیرا که پروتکل‌های مسیریابی امن، بیشتر بر امنیت نگه‌داری مسیر و دفاع در برابر تغییر اطلاعات مسیریابی متمرکز می‌شوند. بنابراین علی‌رغم وجود پروتکل مسیریابی امن برای MANET، ارائه‌ی سرویس گمنامی توسط پروتکل مسیریابی در راستای مقابله با حملات تحلیل ترافیک به منظور پنهان نمودن اطلاعاتی مثل هویت گره‌های شبکه و توپولوژی شبکه الزامی است.

پروتکل‌های مسیریابی گمنام باید به گونه‌ای طراحی شوند که علی‌رغم آن‌که هدایت بسته‌ها در شبکه همانند سابق صورت می‌گیرد، اطلاعات موردنظر از دید مهاجم و در شرایطی حتی از دید گره‌های مجاز شبکه، مخفی بمانند. به این معنا که مثلاً گره‌های میانی یک مسیر بین دو گره‌ی در حال ارتباط، در عین حال که قادرند بسته‌های مبادله شده بین مبدأ و مقصد را به خوبی هدایت کنند، قادر به شناسایی هویت گره‌های مبدأ و مقصد نخواهند بود و در نتیجه گمنامی گره‌های انتهایی فراهم می‌گردد. همچنین به دلیل محدودیت منابع در MANET، کاهش سربار محاسباتی در عین برقراری مسیر به صورت گمنام، از دغدغه‌های اصلی طراحی پروتکل‌های مسیریابی گمنام به شمار می‌آید.

---

[1] Privacy

در واقع در روند طراحی یک پروتکل مسیریابی گمنام باید اصولی مدنظر قرار گیرند. برخی از این اصول عبارتند از: فراهم نمودن چهار جنبه‌ی حریم خصوصی موبایل که امکان نقض آن‌ها در فرآیند مسیریابی وجود دارد یعنی حریم محتوا، حریم شناسه، حریم مکان و حریم مسیر، تقاضامحور بودن پروتکل به منظور پویا بودن اطلاعات مسیریابی و اجتناب از عملیات رمزنگاری حجیم.

در این پایان‌نامه حملات تحلیل ترافیک و شیوه‌های مقابله با آن‌ها در MANET مورد بررسی دقیق قرار می‌گیرند. همچنین پروتکل‌های مسیریابی گمنام مطرح، به عنوان یکی از راهکارهای مقابله با حملات تحلیل ترافیک بررسی شده و پروتکل‌های مسیریابی گمنام پیشنهاد شده، مورد مطالعه و ارزیابی قرار می‌گیرند. در ادامه‌ی این فصل، ابتدا در بخش ۱-۲ انگیزه و اهمیت بحث حملات تحلیل ترافیک تبیین می‌گردد. پس از آن در بخش ۱-۳ مروری بر اهم تحقیقات انجام شده در حوزه‌ی حملات تحلیل ترافیک در MANET ارائه خواهد شد و مهمترین نوآوری‌های پیشنهادی در این پایان‌نامه به اختصار بیان می‌شود. سپس، در بخش ۱-۴ ضمن تشریح ساختار پایان‌نامه، رئوس کلی مطالب مورد بررسی در فصل‌های آینده معرفی خواهند شد.

۱-۲ انگیزه و اهمیت بحث

ویژگی‌ها و قابلیت‌های منحصر به فرد شبکه‌های اقتضایی سیار مثل قابلیت خود سازماندهی و خود نگه‌داری آن‌ها، امکان بکارگیری روزافزون این شبکه‌ها را در کاربردهای مختلفی از جمله کاربردهای نظامی و شهری فراهم نموده است. بسیاری از این کاربردها مانند عملیات میدان جنگ و تجارت الکترونیک، از نظر امنیتی حساس می‌باشند، این در حالی است که مشخصات خاص MANET، مانند بستر ارتباطی بی‌سیم امکان استراق سمع ترافیک مبادله شده و در نتیجه حمله‌ی تحلیل ترافیک را برای مهاجم فراهم می‌آورد. هدف مهاجم از حمله‌ی تحلیل ترافیک به دست آوردن اطلاعاتی چون هویت طرفین ارتباطات، الگوی ترافیک و تغییرات آن است. نشت چنین اطلاعاتی معمولاً مخرب سناریوهای حساس امنیتی است. به عنوان نمونه یک تغییر غیرمنتظره در الگوی ترافیک شبکه‌ی نظامی می‌تواند نشان‌دهنده‌ی شروع اجرای زنجیره‌ی دستورات[1] نظامی باشد. همچنین ممکن است مکان مراکز صدور فرمان یا مکان افراد ویژه در شبکه نظامی برای افراد غیرمجاز آشکار شود.

با این توضیحات واضح است که کشف اطلاعات مفید و حساس در مورد ترافیک شبکه و کاربران آن یا به طور کلی نقض حریم خصوصی، هدف اولیه‌ی مهاجم در حمله‌ی تحلیل ترافیک است. حریم خصوصی در شبکه‌های MANET جنبه‌های متفاوت و جدیدی علاوه بر جنبه‌های سنتی حریم خصوصی در شبکه‌های مبتنی بر زیرساخت دارد. انواع حریم خصوصی در MANET را می‌توان به صورت حریم محتوای پیام، شناسه‌ی گره‌ها، توپولوژی

[1] The chain of commands