Journal of Emerging Defense Knowledge and Research

Volume 1, Issue 1
April 2024
p.p 27-50

Shahid Sattari Air University

Introducing a Hybrid Method to Keep Users Anonymous on the Internet of Things

Amir Mahdi Sazdar[1], Mahmoud Vaseli Khabbaz[2]

Abstract

Background and Purpose: On the Internet of Things (IoT), the anonymity and availability of nodes and the security of the exchanged information have paramount importance. To solve these problems, the combination of methods and technologies introduced in other networks can be used. In this paper, the mechanism of Delay Tolerant Networks (DTN) will be used in order to always save the availability of information. In the next step, in order to ensure anonymity, an improved combination of blockchain technology and anonymous onion routing methods will be used to protect the privacy and security of the information.

Methodology: The present study is presented using methods based on simulation and its implementation in the laboratory environment.

Findings: The proposed method uses the existing infrastructure in the network, as well as to tolerating delays, completely preserves the anonymity of the nodes. The proposed method reduces the computational overload on nodes by promoting onion anonymity methods, and also leads to complete anonymity and direct use in DTN by improving the method of using blockchain technology.

Conclusion: The proposed method, using environmental infrastructure, can be used in DTN and increases the availability of nodes. In addition, applying the mechanism of blockchain systems using the methods of combined services and shared wallets increases the security of data and information measured by IoT equipment and devices.

Keywords: *Internet of things, Network anonymity, Security, Block chain, Onion routing.*

[1] Electronic and Computer Faculty, Shahid Beheshti University, Tehran, Iran.
[2] Malek Ashtar University of Technology, Tehran, Iran.

Received: 2022/04/16
Accepted: 2022/05/22
Corresponding Author :Amir Mahdi Sazdar

فصلنامهٔ سیاستگذاری دانش و پژوهش‌های نوین دفاعی
دوره ۱، شماره ۱
اردیبهشت ۱۴۰۳
صص۲۷-۵۰

معاونت پژوهش و فناوری

ارائه روشی ترکیبی برای حفظ گمنامی کاربران در شبکهٔ اینترنت اشیاء

امیرمهدی سازدار[۱]، محمود واصلی خباز[۲]

چکیده

زمینه و هدف: در شبکه اینترنت اشیاء (IoT) در دسترس بودن همیشگی گره‌ها، وجود گمنامی و تأمین امنیت اطلاعات مبادله شده از اهمیت بالایی برخوردار است. برای حل این مشکلات می‌توان از ترکیب روش‌ها و فن‌آوری‌های معرفی شده در سایر شبکه‌ها استفاده نمود. در این پژوهش به‌منظور در دسترس بودن همیشگی اطلاعات از سازوکار شبکه‌های با تحمل تأخیر بالا (DTN) استفاده خواهد شد. در گام بعد به‌منظور تأمین گمنامی برای حفظ حریم‌خصوصی و امنیت اطلاعات مبادله شده از ترکیب بهبودیافته فن‌آوری زنجیرهٔ بلوکی و روش‌های گمنامی مسیریابی پوست‌پیازی استفاده خواهد شد.

روش‌شناسی: پژوهش حاضر با استفاده از روش‌های مبتنی بر شبیه‌سازی و اجرای آن در محیط آزمایشگاهی ارائه شده است.

یافته‌ها: روش پیشنهادی با استفاده از زیرساخت‌های موجود در شبکه علاوه بر تحمل تأخیر، گمنامی گره‌ها را به‌طور کامل حفظ می‌کند. روش پیشنهادی با ارتقای روش‌های گمنامی پوست پیازی باعث کاهش بار محاسباتی در گره‌ها شده و همچنین با بهبود روش استفاده از فناوری زنجیرهٔ بلوکی به گمنامی کامل و استفاده مستقیم در شبکه‌های با تحمل تاخیر منجر می‌شود.

نتیجه‌گیری: روش پیشنهادی با استفاده از زیرساخت‌های محیطی امکان استفاده در شبکه‌های با تحمل تأخیر را داشته و دسترس‌پذیری گره‌ها را افزایش می‌دهد. به‌علاوه به‌کارگیری سازوکار سیستم‌های زنجیرهٔ بلوکی با استفاده از روش‌های سرویس‌های ترکیب‌کننده و کیف پول اشتراکی باعث افزایش امنیت داده‌ها و اطلاعات سنجیده شده توسط تجهیزات و دستگاه‌های اینترنت اشیاء می‌شود.

کلیدواژه‌ها: *اینترنت اشیاء، گمنامی در شبکه، امنیت، زنجیرهٔ بلوکی، مسیریابی پوست‌پیازی.*

---

۱ دانشکده مهندسی برق و کامپیوتر، دانشگاه شهید بهشتی، تهران، ایران.
۲ دانشگاه صنعتی مالک اشتر، تهران، ایران.

تاریخ دریافت مقاله: ۱۴۰۱/۰۱/۲۷
تاریخ پذیرش نهایی مقاله: ۱۴۰۱/۰۳/۰۱
نویسنده مسئول مقاله: امیرمهدی سازدار

مقدمه

اینترنت اشیاء[1] یکی از فن‌آوری‌های محبوب جهان امروز است که جهان صنعتی و علمی توجه خاصی به آن دارند. از این فن‌آوری در امور مختلفی مانند پایش وضعیت سلامت افراد[2]، شهر هوشمند[3]، صنایع تولیدی و ... استفاده فراوانی می‌شود. داده‌های تولیدشده توسط اشیای مختلف، ارزش و اهمیت تجاری بسیار بالایی برای شرکت‌ها دارند (کواسییم[4]، ۲۰۱۸). اما در مواقعی ارتباط مستقیم این دستگاه‌ها با اینترنت مختل می‌شود. این مشکل انگیزه‌ی ایجاد بستری امن و قابل‌اطمینان برای مخابره و ارسال این بسته‌ها از مبدأ تا مقصد می‌شود تا امکان شنود آن‌ها توسط افراد غیرمجاز به حداقل برسد. از طرف دیگر، از گذشته تا به امروز مواردی مانند عدم آزادی مطبوعات در بسیاری از کشورها، پایش جستجوها و رفتار افراد توسط سازمان‌های بزرگ (مانند گوگل، فیس‌بوک و ...) به‌منظور کشف علایق و ویژگی‌های شخصیتی کاربران و همچنین سایر نمونه‌های نقض حریم شخصی افراد، اهمیت استفاده از روش‌های گمنامی در شبکه‌های ارتباطی را پر رنگ‌تر می‌سازند. به همین دلیل همواره راه‌های مختلفی برای تأمین گمنامی افراد ابداع‌شده‌اند (اوجها[5]، ۲۰۱۶). یکی دیگر از مسائل موجود که همواره موردتوجه محققان و صنایع بوده، شبکه باتحمل تأخیر[6] بالا می‌باشند (جانگ[7]، ۲۰۱۴). شبکه باتحمل تأخیر شبکه‌هایی هستند که توانایی رساندن پیام باوجود قطع شدن‌های مکرر در شبکه را دارند (ساکای[8]، ۲۰۱۷).

برای بیان ارتباط این دو موضوع با یکدیگر می‌توان ارتباطات در میدان نبرد را نام برد. در این نوع ارتباطات علاوه بر حصول اطمینان از دریافت پیام‌ها، می‌توان با رمزنگاری نقطه‌به‌نقطه امنیت محتوای پیام را تأمین کرد. ولی به‌جز محتوای پیام، مخفی نمودن هویت و موقعیت فرستنده و گیرنده نیز از درجه اهمیت بالایی برخوردار است، تا حدی که به مخاطره افتادن و افشای هریک از این موارد می‌تواند باعث شکست در عملیات شود (ساکای، ۲۰۱۷).

با به وجود آمدن فن‌آوری‌های جدید مانند زنجیرهٔ بلوکی انقلاب بزرگی در عرصه اینترنت

---

[1] Internet of Things(IoT)
[2] Health Care
[3] Smart City
[4] Kouicem
[5] Ojha
[6] Delay Tolerant Networks(DTN)
[7] Jung
[8] Sakai

اشیاء صورت گرفت (فاریس[1]، ۲۰۲۱). در این مقاله، با بهره‌گیری از مزایای موجود در مفاهیم زنجیره‌های بلوکی و روش‌های گمنامی موجود، ساختاری جدید برای حفظ گمنامی در شبکهٔ اینترنت اشیاء با توانایی تحمل تأخیر معرفی می‌شود. در ابتدا روش‌های مختلف موجود گمنامی در شبکه‌های ارتباطی شرح داده می‌شود. سپس با استفاده از ترکیب این روش‌ها بستری امن برای تبادل اطلاعات اینترنت اشیاء پیشنهاد داده خواهد شد.

ساختار مقاله حاضر به این شرح است: در بخش بعد ابتدا مرور مختصری بر کارهای انجام‌شده در حوزه امنیت اینترنت اشیاء و مسیریابی در این شبکه‌ها بیان می‌شود و سپس مقدمه‌ای کوتاه از زنجیره بلوکی مطرح می‌شود. در بخش سوم روش پیشنهادی معرفی و در بخش چهار نتایج شبیه‌سازی‌ها آمده و مقایسه روش پیشنهادی با نمونه‌های مشابه بیان می‌گردد و در بخش آخر نتیجه‌گیری آمده است.

پیشینهٔ پژوهش

در این بخش مروری بر فعالیت‌های حوزه امنیت در اینترنت اشیاء و مسیریابی در این شبکه‌ها آمده است و سپس مقدمه‌ای از زنجیره بلوکی مطرح می‌شود.

۲-۱- امنیت در اینترنت اشیاء

در دید کلی، به‌منظور تأمین امنیت اینترنت اشیاء باید سرویس‌هایی از قبیل محرمانگی[2] (ایجاد اطمینان از عدم دسترسی افراد غیرمجاز به اطلاعات صحیح)، اطمینان از صحت[3] (اطمینان از عدم دست کاری داده توسط افراد دیگر)، احراز هویت[4] (اطمینان از هویت منبع)، انکارناپذیری[5] (منبع داده‌ها امکان انکار پیام را نداشته باشد)، در دسترس بودن[6] (ایجاد اطمینان از در دسترس بودن سرویس مورد نیاز) و ایجاد حریم خصوصی[7] (اطمینان از عدم افشای اطلاعات منبع) را تأمین کرد (کواسییم، ۲۰۱۸). البته شایان‌ذکر است که در کاربردهای مختلف اینترنت اشیاء، اهمیت سرویس‌های فوق متفاوت است. برای مثال در فرایندهای مالی صحت و احراز هویت افراد، در سفارش‌های اینترنتی انکارناپذیری و در پایش وضعیت سلامت افراد، احترام به حریم خصوصی بیمار اهمیت بسیار زیادی دارد. از طرف

---

[1] Faris
[2] Confidentiality
[3] Integrity
[4] Authentication
[5] Non-repudiation
[6] Availability
[7] Privacy

دیگر وسایل هوشمند اکثراً کوچک بوده و در منابع انرژی[1]، پردازشی[2] و حافظه[3] محدودیت‌هایی دارند. پس استفاده از الگوریتم‌های رمزنگاری پیچیده در آن‌ها کار معقولی نیست (کواسییم، ۲۰۱۸).

۲-۲- روش‌های گمنامی

به‌منظور ایجاد گمنامی در شبکه، راه‌حل‌های مختلفی با کمک سرویس‌دهنده‌های گمنامی و یا رویکردهای مشارکتی و گروهی ارائه‌شده است. به‌عنوان نمونه یکی از پرکاربردترین روش حفظ گمنامی با استفاده از سرویس‌دهنده‌ها به کمک سیاست‌گذاری انجام می‌شود. در این روش، گمنامی توسط سیاست‌گذاری‌های شرکت ثالث تأمین می‌شود. کاربر باید در زمان شروع استفاده از سرویس‌های این سازمان‌ها، سیاست‌های آن‌ها را بپذیرد. ولی سازمان در هرلحظه مختار به تغییر سیاست‌گذاری‌های خود بوده و کسی حق شکایت ندارد (اوجها، ۲۰۱۶). روش دیگر گمنامی به وسیله طراحی است. در این نوع گمنامی، گمنامی به‌عنوان سرویس بدون هیچ قانونی، به کاربران ارائه می‌شود. برای مثال می‌توان استفاده از سرویس‌دهنده‌ی پروکسی[4] را نام برد. در این روش تمام ترافیک کاربر از کانال سرویس‌دهنده‌ی پروکسی با مقصد ردوبدل می‌شود. از دید کاربر، با سرویس‌دهنده‌های وب مختلف در ارتباط است ولی از دید مقصد مبدأهای مختلفی مشاهده می‌شود. مختل شدن تک نقطه‌ای و دانستن تمامی اطلاعات توسط سرویس‌دهنده‌ی پروکسی از معایب این روش است (اوجها، ۲۰۱۶). از نمونه روش‌های مشارکتی برای حفظ گمنامی می‌توان به استفاده از روش‌های تودرتو یا به اصطلاح پیازی و یا زنجیره بلوکی اشاره نمود، که در ادامه به معرفی بیشتر آن‌ها پرداخته می‌شود.

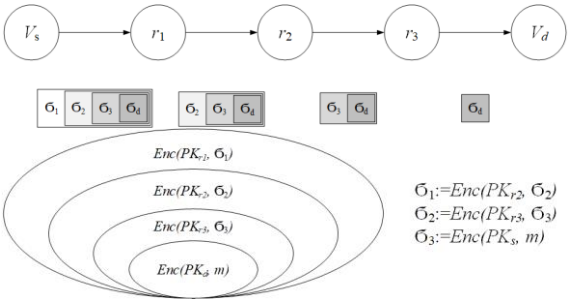
۲-۲-۱- مسیریابی پیازی[5]

در این روش، محتوا و هویت فرستنده و گیرنده به‌صورت کامل حفظ می‌شود. فرستنده در ابتدا مسیری مجازی متشکل از چندین گره واسط تشکیل داده و با آن‌ها تبادل کلید انجام می‌دهد (اوجها، ۲۰۱۶). سپس پیام خود را با استفاده از کلیدها به ترتیب از دورترین به نزدیک‌ترین گره رمزنگاری کرده و سپس به اولین گره می‌فرستد. گره اول بسته را

---

[1] Power Resource
[2] Processing
[3] Memory
[4] Proxy Server
[5] Onion Routing

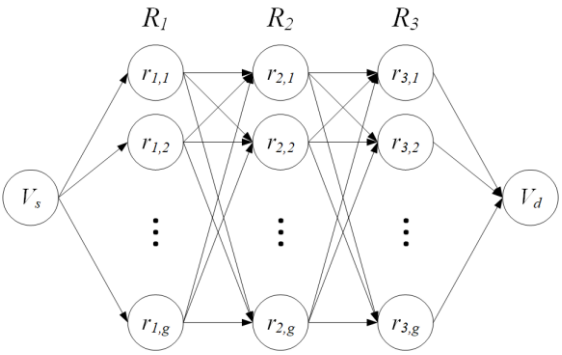
رمزگشایی و آدرس گره دوم را به دست می‌آورد تا بتواند آن را برای گره دوم ارسال کند. بـه همین ترتیب هر گره فقط امکان رمزگشایی لایه‌ی مربوط به خـود را داشـته و فقـط از گـره قبلی و بعدی خود اطلاع دارد. از دیدگاه مقصد، فرستنده پیـام آخـرین گـره‌ی عضـو شـبکه مسیریابی پیازی است. شکل ۱ نشان‌دهنده روش رمزنگاری و ارسـال اطلاعـات از مبـدأ بـه مقصد است. به دلیل این ساختار رمزنگاری لایه‌ای، نـام ایـن روش مسـیریابی پیـازی اسـت (ساکای، ۲۰۱۷).



شکل ۱. نمونه مسیریابی پیازی، ارسال داده از مبدأ v_s به مقصد v_d (ساکای، ۲۰۱۷)

با ایجاد تغییراتی در مسیریابی پیازی و معرفی مسیریابی پیازی گروهی، می‌تـوان از آن در شبکه‌ها باتحمل تأخیر، به‌منظور ایمن‌سازی ارتباط، استفاده کرد (ساکای، ۲۰۱۷). با توجـه به این نکته که در این نوع شبکه‌ها امکان قطع ارتباط هر یک از گره‌هـا در هرلحظـه وجـود دارد و در مسیریابی پیازی، هر لایه فقط با کلید خصوصی یک گره خاص باز مـی‌شـود، بایـد تغییراتی در ساختار مسیریابی پیازی ایجاد گردد (سـاکای، ۲۰۱۷). مشـابه آنچـه در شـکل ۲ آمده است، برای تحقق این منظور، گره‌های مختلف باهم تشکیل گروه داده و جفت کلیـد[1]، درون گروه به اشتراک گذاشته می‌شود. هر گـره عضـو گـروه خـاص، تـوان انجـام عملیـات رمزنگاری و رمزگشایی مربوط به آن گروه را دارد (ساکای، ۲۰۱۷).

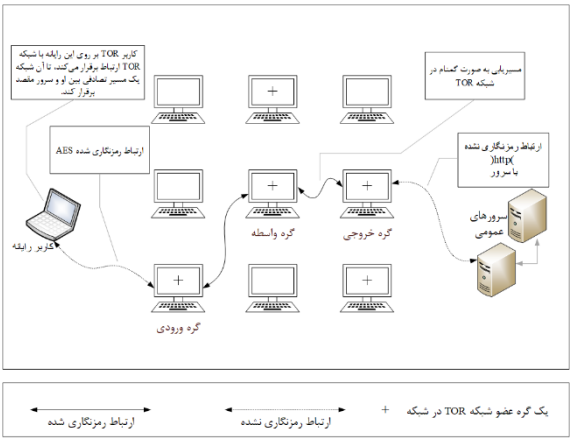
[1] Key-Pair



شکل ۲. یک گروه g عضوی در مسیریابی پیازی گروهی (ساکای، ۲۰۱۷).

به‌منظور افزایش کارایی و اطمینان از رسیدن پیام به مقصد، در این شبکه‌ها چندین نسخه از هر داده از طریق مسیرهای مختلف فرستاده می‌شود. البته افزایش تعداد نسخه‌ها با کاهش امنیت نسبت مستقیم دارد، پس باید در انتخاب تعداد نسخه‌های مجاز، بین امنیت و کارایی تعادل ایجاد کرد (ساکای، ۲۰۱۷).

شبکه TOR[1] نسخهٔ دوم مسیریابی پیازی است. این شبکه دادهٔ کاربر را حداقل از سه سرویس‌دهنده (ورودی، واسط و خروجی) عبور می‌دهد. همانطور که در شکل ۳ مشاهده می‌شود، می‌توان تعداد سرویس‌دهنده‌های واسط را افزایش داد، ولی به‌منظور کاهش تأخیر شبکه، یک سرویس‌دهنده واسط توصیه می‌شود (اوجها، ۲۰۱۶).

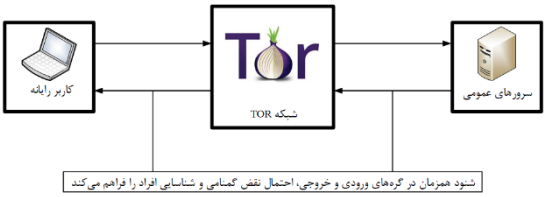


شکل ۳. نحوه کار شبکه TOR (اوجها، ۲۰۱۶)

[1] The Onion Routing

در این شبکه، به‌منظور ایجاد کمترین تأخیر و بیشترین سرعت ممکن، از بین سرویس‌دهنده‌های خروجی، سرویس‌دهنده‌ای که ازنظر معیارهایی مانند ظرفیت انتقال اطلاعات و زمان در دسترس بودن ممتد در شبکه[1] برتری نسبی داشته باشد، انتخاب می‌شود. همچنین برای کاهش تأخیر، به‌صورت پیش‌فرض در هر ۳۰ ثانیه یک مدار مجازی جدید تشکیل می‌شود و ارتباطات TCP جدید از آن عبور داده می‌شود. به‌منظور افزایش امنیت، هر ارتباط TCP به‌صورت پیش‌فرض بیشتر از ۱۰ دقیقه بر روی یک مدار مجازی نمی‌ماند و بعد از پایان این زمان مدار عوض می‌شود (ایشان[2]، ۲۰۲۱).

تحقیقات نشان می‌دهد باوجود تعداد زیادی سرویس‌دهنده خروجی برای این شبکه، از بخش اندکی از آن‌ها استفاده می‌شود. وجود قوانین بازدارنده در بعضی از کشورها، انتخاب سریع جهت کاهش زمان انتخاب سرویس‌دهنده خروجی (کوخ[3]، ۲۰۱۶) و همچنین معیارهای انتخاب سرویس‌دهنده خروجی در این شبکه، دلایل اصلی این امر هستند (اوجها، ۲۰۱۶). از طرفی انجام کارهای غیرقانونی با استفاده از بستر این شبکه، باعث شده سازمان‌های امنیتی به کمک سازمان‌ها و شرکت‌های زیرساختی اقدام به شنود و بررسی ترافیک این شبکه‌ها کنند (کوخ، ۲۰۱۶). استفاده از سرویس‌دهنده‌های خروجی محدود باعث می‌شود این سازمان‌ها با استفاده از شنود گسترده و بررسی ترافیک ورودی و خروجی شبکه TOR، مانند شکل ۴، احتمال شناسایی کاربر را داشته باشند (اوجها، ۲۰۱۶).

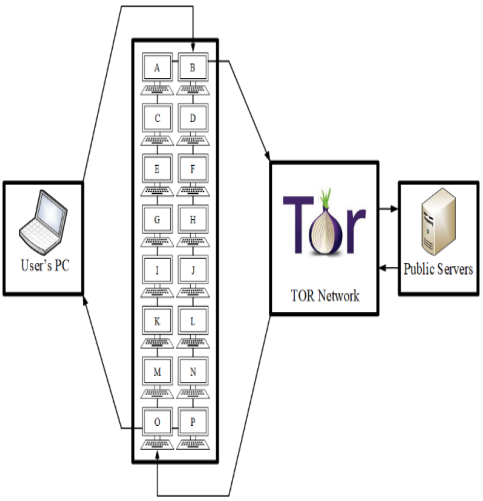


شکل ۴. نحوه شنود شبکه توسط سازمان‌های بزرگ (اوجها، ۲۰۱۶)

راه‌حل پیشنهادی، مشابه آنچه در شکل ۵ نشان داده شده، استفاده از یک‌لایه‌ی میانی به نام AEL[4] است. با توجه به ارسال درخواست و دریافت پاسخ از طریق دو کامپیوتر مختلف در لایه‌ی میانی، کاربر از خطر شنود، در امان می‌ماند. روش کار این لایه در الگوریتم (۱) آمده است (اوجها، ۲۰۱۶).

---

[1] Uptime
[2] Ishan
[3] Koch
[4] Advanced Encryption Layer



شکل ۵. افزودن لایه‌ی میانی AEL جهت افزایش امنیت (اوجها، ۲۰۱۶)

الگوریتم (۱): نحوه کار الگوریتم لایه‌ی میانی AEL:

۱) در ابتدا کاربر یک کامپیوتر تصادفی از میان کامپیوترهای در لایه‌ی میانی انتخاب کرده و درخواست خود را به آن می‌فرستد.

۲) کامپیوتر انتخابی درخواست رمزنگاری‌شده‌ای دریافت می‌کند که به محتوای اصلی آن دسترسی ندارد. این گره حتی مقصد نهایی را نیز نمی‌داند. این کامپیوتر با استفاده از آدرس فرستنده یک خلاصهٔ درهم‌سازی[1] شده ایجاد می‌کند که به ازای هر درخواست، یکتا است. سپس یک مدار TOR تشکیل می‌دهد.

۳) وقتی شبکه TOR جواب را برمی‌گرداند، یکی از کامپیوترهای عضو AEL به صورت تصادفی انتخاب شده، جواب را دریافت کرده و مسئولیت ارسال این جواب به کاربر اصلی را بر عهده می‌گیرد. ولی برای انجام این کار به آدرس فرستنده نیاز دارد.

۴) آدرس کاربر درون مقدار درهم‌سازی شده‌ی موجود در جواب ارسالی از شبکه وجود دارد. این درهم‌سازی در میان کامپیوترهای لایه AEL منتشرشده، تا آدرس فرستنده بازیابی شود.

۵) وقتی آدرس بازیابی شد، پاسخ شبکه به آن فرستنده می‌شود.

۲-۲-۲- فن‌آوری زنجیرهٔ بلوکی

زنجیرهٔ بلوکی یک فن‌آوری امن، نظیر به نظیر۲ و غیرمتمرکز۳ است (مبارک۴، ۲۰۱۷). از این فناوری در زمینه‌ها و سرویس‌های گوناگون مانند بازار مالی، اینترنت اشیاء و .... استفاده

---

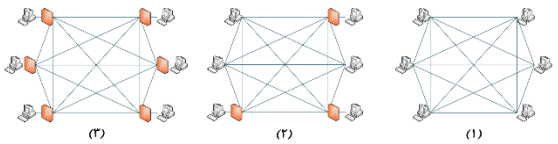
[1] Hash
[2] Peer-to-Peer
[3] Distributed
[4] Mobarak

می‌شود (لین[1]، ۲۰۱۷). اکثر فن‌آوری‌های زنجیرهٔ بلوکی متن‌باز هستند. همچنین خصوصیاتی چون گمنامی گره‌ها، مقاوم بودن در برابر خطا و امنیت بالای داده‌های ذخیره‌شده در بلاک‌ها در برابر تخریب آن را تبدیل به یک فن‌آوری امن کرده است (لـین، ۲۰۱۷). از معـروف‌تـرین مثال‌های این فن‌آوری می‌توان به بیت‌کوین[2]، اتریوم[3] و Hyperledger اشاره کرد (مبارک، ۲۰۱۷). نحوه کار زنجیرهٔ بلوکی به‌صورت مراحل الگوریتم (۲) است.

الگوریتم (۲): نحوه کار زنجیرهٔ بلوکی (لین، ۲۰۱۷)

۱) گره ارسال‌کننده اطلاعات ارسالی را در شبکه پخش می‌کند.
۲) گره دریافت‌کننده در ابتدا پیام داخل بستهٔ داده را بررسی کرده و در صورت تأیید اطلاعات، آن را در یک بلاک ذخیره می‌کند.
۳) همهٔ گره‌های دریافت‌کننده، الگوریتم‌های تصدیق کار یا تصدیق سهام را برای این بلاک اجرا می‌کنند.
۴) این بلاک بعد از پایان اجرا الگوریتم اجماع جمعی مرحله قبل، در زنجیره بلاک‌ها ذخیره می‌شود.

بـه گـره‌هـایی کـه در زنجیـرهٔ بلـوکی منـابع محاسـباتی خـود را بـه‌منظـور محاسـبه الگوریتم‌های پیچیده تصدیق کار یا تصدیق سهام و تولید بلاک‌ها، بـه اشـتراک مـی‌گذارنـد، کاوشگر[4] گویند (رومی[5]، ۲۰۲۱). همان‌گونه که در شکل ۶ آمده است، زنجیرهٔ بلوکی‌ها ازنظر نوع ساختار به سه نوع عمومی، ائتلافی[6] و خصوصی دسته‌بندی مـی‌شـوند (لـین، ۲۰۱۷). در حالت عمومی، مانند بیت‌کوین و اتریوم، همه اعضاء می‌توانند در فرایند زنجیرهٔ بلوکی شرکت کنند. در حالت ائتلافی، مانند Hyperledger، گره‌هایی که اجازه دسترسی دارنـد مـی‌تواننـد مجوز شرکت یا عدم شرکت سایر گره‌ها را صادر کند. در این سیسـتم‌هـا داده مـی‌توانـد بـه حالت امن و یا معمولی جابه‌جا شود. در حالت خصوصی، تنها گره‌های مشخص اجازه شـرکت داشته و داده به‌صورت امن بین آن‌ها جابه‌جا می‌شود (جوشی[7]، ۲۰۱۸).



شکل ۶. انواع مختلف زنجیرهٔ بلوکی ازنظر ساختار؛(۱) عمومی، (۲) ائتلافی ، (۳) خصوصی (لین، ۲۰۱۷)

---

[1] Lin
[2] Bitcoin
[3] Ethereum
[4] Miner
[5] Romi
[6] Consortium
[7] Joshi

در این فن‌آوری مشکل گمنامی به‌واسطه اعتماد متقابل گره‌ها به همدیگر حل می‌شود؛ به صورتی که هر گره برای انتقال داده به گره دیگر تنها نیازمند دانستن آدرس زنجیرهٔ بلوکی آن گره بوده و به آدرس حقیقی آن نیازی ندارد (لین، ۲۰۱۷).

به‌عنوان مثال کاربردی برای این فن‌آوری، می‌توان از آن برای حل مسائل جمع‌حسی[1] کمک گرفت. در این نوع از مسائل، داده‌های خاصی با استفاده از حس‌گرهای دستگاه‌های موجود جمع‌آوری می‌شود. به‌منظور افزایش کیفیت اطلاعات جمع‌آوری‌شده، باید با دستگاه‌های قوی‌تر موجود در منطقه، همکاری لازم انجام شود. به‌منظور افزایش امنیت و همچنین ایجاد انگیزه برای آن دستگاه‌ها، می‌توان توسط ساختار زنجیرهٔ بلوکی، با توجه به میزان همکاری آن‌ها، جوایزی را به آن‌ها تخصیص داد (وانگ[2]، ۲۰۱۸).

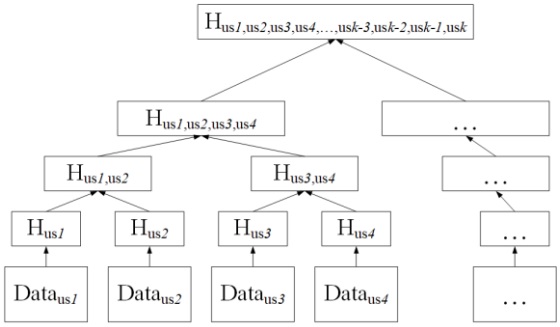
در فناوری زنجیرهٔ بلوکی به‌منظور تبادل اطلاعات و انجام تراکنش، فقط آدرس اختصاصی زنجیرهٔ بلوکی گره‌ها لازم بوده و آدرس اینترنتی[3] آن‌ها از دید یکدیگر پنهان می‌ماند (وانگ، ۲۰۱۸). به دلیل وجود همین ویژگی در این فن‌آوری، گمنامی افراد تا حد زیادی حفظ‌شده و اصطلاحاً یک شبه‌گمنامی[4] به وجود می‌آورد (سان[5]، ۲۰۱۹). باوجود استفاده از آدرس‌های زنجیرهٔ بلوکی، بازهم درنهایت گره‌ها قابل‌ردیابی هستند، زیرا هر گره برای تولید آدرس زنجیرهٔ بلوکی، نیاز به ورود اطلاعات شخصی خود در یک سرویس‌دهنده دارد. به همین منظور از اصطلاح شبه‌گمنامی استفاده‌شده است (موزر، ۲۰۱۳). با توجه به اینکه در کاربردهایی مانند کاربرد جمع‌حسی، یا پایش وضعیت سلامت افراد اطلاعات حساسی از حس‌گرهای گره‌ها جمع‌آوری می‌شود، باید امنیت این داده‌ها را افزایش داده و به گره‌ها اطمینان کافی داد که حتی از طریق آدرس زنجیرهٔ بلوکی نیز، قابل‌ردیابی نیستند.

برای حل این مشکل در مقالات مختلف راه‌حل‌های گوناگونی پیشنهادشده است. به‌عنوان نمونه، می‌توان بجای اینکه هر گره، داده‌های خود را به‌صورت مستقیم به شبکه زنجیرهٔ بلوکی ارسال کند، گروه‌هایی k تایی از گره‌ها به وجود آورد که این گره‌ها به هم اعتماد کامل داشته باشند. سپس داده‌های داخل این گروه‌ها به روش درخت مرکل[6]، نمایش داده‌شده در شکل ۷، درهم‌سازی شده و سپس توسط یکی از اعضای گروه، که هر دفعه به‌صورت تصادفی انتخاب می‌شود، به شبکه زنجیرهٔ بلوکی فرستاده شود. به‌واسطه این روش،

---

[1] Crowd-sensing
[2] Wang
[3] Internet Protocol (IP)
[4] Pseudonymity
[5] Sun
[6] Merkle Tree

چون در هر نوبت داده‌های درهم‌سازی شده، از دید شبکه زنجیرهٔ بلوکی توسط افراد مختلفی ارسال می‌شوند، پس در این صورت یک k–گمنامی[۱] نیز برای هر گره ایجاد می‌شود (وانـگ، ۲۰۱۸).

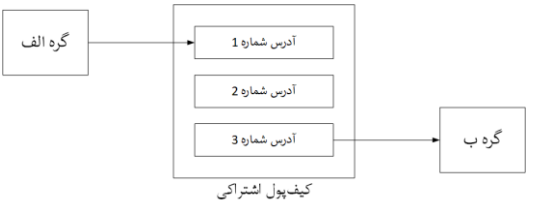


شکل ۷. سازوکار درخت مرکل (وانگ، ۲۰۱۸)

در راه‌حل دوم، برای افزایش گمنامی گره‌ها و قطع اتصال بین آدرس زنجیرهٔ بلوکی هر گره با مشخصات اصلی آن، می‌توان از سرویس‌های ترکیب کـردن[۲] اسـتفاده کـرد (مـوزر[۳]، ۲۰۱۳). این سرویس‌ها، برای گم کردن رد تراکنش‌ها، تراکنش چند کـاربر مختلـف را بـاهم ترکیب می‌کنند. درنتیجه این کار تحلیل ورودی و خروجی به‌منظور کشف گـره‌هـا، دشـوارتر می‌شود. در این راه‌حل ممکن است خود سرویس‌دهنده، قصد شنود داشـته باشـد و گمنـامی طرفین به خطر می‌افتد که راه‌حل آسان آن استفادهٔ چندلایه‌ای از این سرویس‌هـا اسـت بـه صورتی که خروجی یک سرویس خود ورودی سرویس بعدی باشد. در این صورت هیچ‌کـدام از سرویس‌دهنده‌ها به‌تنهایی هر دو طرف تراکنش را نمـی‌شناسـند. پیـاده‌سـازی ایـن روش به‌صورت سنتی به‌منظور دریافت و ارسال اطلاعات رمزنگاری‌شده در سیستم‌های مالی ماننـد بیت‌کوین امکان‌پذیر نیست. زیرا تراکنش باید در زنجیرهٔ بلوکی ثبت شود با فرستنده امکـان خرج کردن دوباره[۴] همان پول را نداشته باشد. به همین منظـور سـرویس‌دهنـده‌هـایی ماننـد Blockchain.info این سرویس را با استفاده از روش کیف پول اشتراکی[۵]، ارائه مـی‌دهنـد. روش کار این سرویس‌ها که در شکل ۸ نشان داده شده، به این صورت است کـه ابتـدا گـره اول تـراکنش خـود را بـا یکـی از آدرس‌هـای سـرویس‌دهنـده انجـام مـی‌دهـد و سـپس

[1] k-Anonymity
[2] Mixing Services
[3] Moser
[4] Double-Spending
[5] Shared-Wallet

سرویس‌دهنده با استفاده از یکی از آدرس‌هایی که در اختیار دارد، این تراکنش را با گرهٔ مقصد انجام می‌دهد (موزر، ۲۰۱۳).



شکل ۸. پنهان سازی ارتباط دو گره را با دو آدرس متفاوت (موزر، ۲۰۱۳)

روش پیشنهادی

باید توجه داشت که در مواقعی اشیای هوشمند موجود، بنا به دلایل مختلف نظیر عدم وجود زیرساخت، اختلال در زیرساخت و یا هر دلیل دیگری امکان اتصال به اینترنت و ردوبدل اطلاعات با سرویس‌دهنده را ندارند. این خود مصداقی از عدم در دسترس بودن گره موردبحث است که خود یکی از موارد نقض ایمنی ذکرشده در بخش ۲ است. علاوه بر این در این موارد پارامتر تاخیر نیز به شدت افزایش می‌یابد. برای ایجاد بستری مناسب و امن، برای انتقال اطلاعات از گره‌های متفاوت تا مقصد، باید موارد متفاوتی را در نظر داشت که در الگوریتم (۳) به‌طور مختصر راه‌حلی بیان‌شده است.

الگوریتم (۳): نحوه کار الگوریتم پیشنهادی

۱) گره با گره‌های مشابه اطراف تشکیل گروه می‌دهد و برای یک کلید مشترک به اجماع می‌رسند.
۲) گرهٔ مبدأ، به‌وسیله کلید عمومی مقصد اطلاعات را رمزنگاری می‌کند و گواهی کلید عمومی خود را در کنار اطلاعات رمزنگاری شده قرار می‌دهد.
۳) گرهٔ مبدأ، به‌وسیله کلید خصوصی مشترک گروه، بسته را امضاء می‌کند و m نسخه از آن را انتشار می‌دهد.
۴) در صورت ارتباط مستقیم با اینترنت بین مرحله ۵ یا ۷ یکی را انتخاب می‌کند، در غیر این صورت به مرحله ۵ می‌رود.
۵) ارسال بسته به یکی از گره‌های هم‌گروهی به صورت تصادفی
۶) گره‌ای دریافت‌کننده به مرحله ۴ الگوریتم می‌روند.
۷) گره یکی از آدرس‌های زنجیرهٔ بلوکی را انتخاب می‌کند.
۸) بسته را به شبکه زنجیرهٔ بلوکی ارسال می‌کند.
۹) مقصد پس از دریافت بسته و تصدیق هویت و رمزگشایی در صورت نیاز به پاسخ به گام بعد می‌رود، در غیر این صورت به گام ۱۵ می‌رود.
۱۰) اطلاعات را با کلید عمومی موجود در بسته رمزنگاری و سپس با کلید خود امضا می‌کند.

۱۱) تعداد s نسخه از طریق زنجیرهٔ بلوکی با سرویس‌های ترکیبی ارسال می‌کند.
۱۲) گره گیرنده اطلاعات را از زنجیرهٔ بلوکی دریافت می‌کند.
۱۳) گره سعی در تصدیق هویت فرستنده و رمزگشایی می‌کند، در صورت عدم موفقیت آن را در گروه انتشار می‌دهد. در صورت موفقیت به گام ۱۵ می‌رود.
۱۴) مرحله ۷ تکرار می‌شود تا اطلاعات به مقصد برسد.
۱۵) پایان

در ادامه به‌صورت جداگانه به بیان جزییات الگوریتم پرداخته خواهد شد. به‌منظور افزایش احتمال اتصال گره‌ها با اینترنت، هر گره با گره‌های مجاور خود با استفاده از ابزارهای ارتباطی مانند بلوتوث یا وای-فای، از طریق اتصال مستقیم دستگاه به دستگاه[1] ارتباط برقرار می‌کند (ژاو[2]، ۲۰۱۶). به‌این‌ترتیب یک گروه k عضوی ایجاد می‌شود که به‌واسطه آن حتی اگر ارتباط مستقیم با اینترنت نیز قطع باشد، گره می‌تواند با ارسال بستهٔ اطلاعات خود به گره‌های دیگر، احتمال دستیابی به اینترنت و رسیدن اطلاعات به مقصد را افزایش دهد. در این روش هر گره حتی در صورت اتصال به اینترنت، حق انتخاب ارسال بسته به اینترنت و یا به گره‌های هم‌گروهی خود را دارد.

ایجاد گروه و ارسال اطلاعات از طریق هم‌گروهی‌ها مشکلاتی از قبیل افشای اطلاعات ارسالی به وجود می‌آورد (ساکای، ۲۰۱۷). برای حل این مشکل از سازوکار رمزنگاری، به روش جفت کلیدهای الگوریتم‌های مبتنی بر خم‌های بیضوی[3] (ECC)، بسته‌های ارسالی استفاده می‌شود. زیرا باید توجه داشت که منابع موجود در اشیاء محدودیت‌هایی دارد و استفاده از الگوریتم ECC با طول کلید ۱۰۲۴ از الگوریتم RSA، حافظه و زمان اجرای کم‌تری لازم داشته و همان سطح امنیتی را دارد (کواسیبیم، ۲۰۱۸). به‌منظور افزایش گمنامی، در داخل گروه، گره‌ها از دو سری جفت کلید استفاده می‌کنند؛ جفت کلیدها شخصی خود گره‌ها و جفت کلید مشترک بین همهٔ اعضای یک گروه. ولی حتی اعضای یک گروه نیز از کلید عمومی شخصی یکدیگر خبری ندارند. گره مبدأ، پس از تشکیل گروه و تبادل کلید، بسته را به صورت رابطه (۱) تولید می‌کند.

$$Sign_{K_{Group}}\left(Enc_{K^{+}_{Destination}}\left(Data \,||\, K^{+}_{Source}\right)\right) \qquad (۱)$$

که در این رابطه K_u^+ و K_u^- به ترتیب کلیدهای عمومی و خصوصی کاربر u و $Sign_K$

[1] Device-to-Device Connection (D2D)
[2] Zhao
[3] Elliptic Curve cryptography

امضا با کلید K است. همان‌طور که مشاهده می‌شود فرستنده اطلاعات ارسالی و کلید عمومی خود را در بسته‌ای قرار داده و توسط کلید عمومی مقصد نهایی رمزنگاری و سپس توسط کلید خصوصی گروه امضاء می‌کند. درنتیجه مقصد نهایی توانایی تصدیق هویت[1] پیام توسط کلید عمومی گروه را دارد.

از آنجا که در این شبکه امکان قطع ارتباط اعضاء در هرلحظه با سایر اعضای گروه وجود دارد، برای ارسال بسته، از سازوکار استفاده‌شده در شبکه‌های باتحمل تأخیر استفاده می‌شود (ساکای، ۲۰۱۷)؛ به این صورت که m نسخه از بسته موردنظر به اعضای مختلف ارسال می‌شود. همه‌ی گره‌ها، حتی گره مبدأ، در صورت اتصال به اینترنت، حق انتخاب بین ارسال آن به بیرون از شبکه داخلی و یا به اعضای گروه را دارد.

برای تأمین گمنامی گروه در شبکهٔ اینترنت و استفاده از تمام زیرساخت‌های موجود، در مرحله ارسال اطلاعات به اینترنت، از سازوکار موجود در فن‌آوری زنجیرهٔ بلوکی استفاده می‌شود و از این طریق اطلاعات از گروه موردنظر برای سرور ارسال می‌شود. در این روش، n آدرس مختلف به‌صورت اشتراکی در اختیار افراد گروه است درنتیجه مانند آنچه در کیف پول‌های اشتراکی (کوخ، ۲۰۱۶) اتفاق می‌افتاد، گمنامی گروه در کل شبکه تأمین می‌شود. در الگوریتم (۴) روش انتقال بسته‌ها آمده است.

الگوریتم (۴): انتقال بسته‌ها
۱) دریافت اطلاعات از هم‌گروهی
۲) در صورت اتصال مستقیم به اینترنت انتخاب یکی از مراحل ۵ و ۳
۳) ارسال بسته به اعضای دیگر گروه
۴) تکرار گام ۲
۵) انتخاب تصادفی یکی از آدرس‌های موجود در زنجیرهٔ بلوکی
۶) ارسال مستقیم به مقصد با استفاده از زنجیرهٔ بلوکی
۷) پایان

مقصد صحت بستهٔ دریافتی را با کلید عمومی گروه که در اختیار دارد بررسی کرده، سپس با کلید خصوصی خود محتوای بسته را باز می‌کند. در گام بعد، برای ارسال جواب به گرهٔ مبدأ پیام، ابتدا آن را به‌وسیله‌ی کلید عمومی گره، که در بسته ارسالی موجود بود، رمز و سپس با کلید خصوصی خود امضاء می‌کند. سپس تعداد s نسخه از آن را به روش زنجیرهٔ

[1] Verify

بلوکی با استفاده از سرویس‌های ترکیب کردن چندلایه (کوخ، ۲۰۱۶)، به آدرس گروه ارسال می‌کند. فرایند انجام روش پیشنهادی در سمت سرویس‌دهنده در الگوریتم (۶) آمده است.

الگوریتم (۶): فرایند روش پیشنهادی در سمت سرویس‌دهنده
۱) دریافت بسته از زنجیرهٔ بلوکی
۲) کنترل صحت امضای بسته
۳) درصورت وجود خطا بسته کنار گذاشته می‌شود و پایان
۴) رمزگشایی بسته بوسیله کلید خصوصی و دریافت اطلاعات
۵) اگر بسته نیاز به پاسخ ندارد برو به پایان
۶) رمزنگاری اطلاعات بوسیله کلید عمومی موجود در بسته
۷) امضاء اطلاعات بوسیله کلید خصوصی
۸) ارسال بوسیله زنجیرهٔ بلوکی و سرویس‌های ترکیب کردن
۹) پایان

گیرنده‌های بسته پاسخ، ابتدا سعی در تصدیق هویت فرستنده و سپس رمزگشایی به‌وسیله کلید خصوصی خود می‌کنند، در صورت عدم موفقیت، آن را برای اعضای دیگر شبکه داخلی انتشار می‌دهند. هر گره دریافت‌کننده دوباره این کار را تکرار می‌کند و در صورت عدم موفقیت، آن را دوباره انتشار می‌کند. از آنجا که بستهٔ پاسخ، توسط کلید عمومی فرستندهٔ اصلی رمزنگاری شده‌اند، تنها گره‌ای امکان رمزگشایی بسته پاسخ را دارد که مقادیر و پیش‌نیازهای آن را فرستاده است.

الگوریتم (۷): نحوه کار گره گیرنده اطلاعات
۱) دریافت بسته پاسخ
۲) تصدیق صحت بوسیله کلید عمومی سرویس‌دهنده در صورت موفقیت آمیز بودن گام بعد در غیر این صورت گام ۵
۳) رمزگشایی بوسیله کلید خصوصی در صورت موفقیعت آمیز بودن گام بعد در غیر این صورت گام ۵
۴) دریافت اطلاعات
۵) انتشار درون شبکه داخلی
۶) پایان

تحلیل کارایی و مقایسه روش پیشنهادی

به‌منظور آنالیز و بررسی روش پیشنهادی، عملکرد گام‌های متفاوت آن را با استفاده از نتایج آزمایش‌های مطرح‌شده در مقالات و نتایج حاصل از آزمایش‌های انجام‌شده توسط

نویسندگان بررسی می‌شود. برای بررسی میزان کارایی گام ایجاد ارتباط گره‌ها و تشکیل گروه، از آنالیزهای موجود در مقاله (جانگ، ۲۰۱۴) استفاده‌شده است. زیرا فقط ماهیت پیام‌ها عوض‌شده و انتقال آن‌ها مانند موارد ذکرشده در مقاله مرجع است.

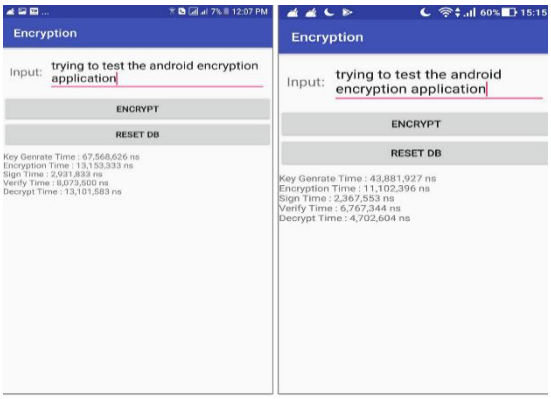
آزمایش مربوطه در (جانگ، ۲۰۱۴)، توسط شبیه‌ساز NS3 در یک محیط ۱۰۰مترمربعی توسط ارتباط وای‌فای مستقیم[1] انجام‌شده است. نتایج حاصل نشان می‌دهد که تبادل انتها به انتهای[2] بسته‌ها (ده هزار بسته) برای یک گروه ۵۰ عضوی به‌طور متوسط تقریباً زمانی برابر ۵۵ میلی‌ثانیه تأخیر[3] دارد. به‌منظور شبیه‌سازی گام رمزنگاری از گوشی‌های هوشمند با سیستم‌عامل اندروید و کتابخانه متن‌باز Themis[4] استفاده‌شده است. مدل‌های استفاده‌شده در این آزمایش، به همراه ویژگی‌هایی مانند منابع حافظه‌ای و پردازشی در جدول ۱ معرفی‌شده‌اند.

جدول ۱. مدل تلفن‌های همراه استفاده شده در طرح و ویژگی‌های سخت‌افزاری آن‌ها

ردیف	مدل تلفن همراه	پردازنده/ حافظه داخلی
۱	Nexus 5	Quad-core 2.3 GHz Krait 400/2^{GB}
۲	Samsung Galaxy Note 4	Quad-core 2.7 GHz Krait 450 - Snapdragon 805/3^{GB}
۳	Huawei P8	Octa-core (4x2.0 GHz Cortex-A53 & 4x1.5 GHz Cortex-A53) /3^{GB}
۴	Asus Zenfon3	Octa-core 2.0 GHz Cortex-A53/3^{GB}
۵	Huawei Honor 8	Octa-core (4x2.3 GHz Cortex-A72 & 4x1.8 GHz Cortex A53) /4^{GB}
۶	Samsung Galaxy Note 5	Octa-core (4x2.1 GHz Cortex-A57 & 4x1.5 GHz Cortex-A53) /4^{GB}
۷	Samsung S8+	Octa-core (4x2.3 GHz Mongoose M2 & 4x1.7 GHz Cortex-A53) /4^{GB}

شکل۹. نمونه‌های از اجرای برنامه روی دو مدل از گوشی‌های هوشمند ایسوز رنفون ۳ و سامسونگ نوت ۳ را نشان می‌دهد.

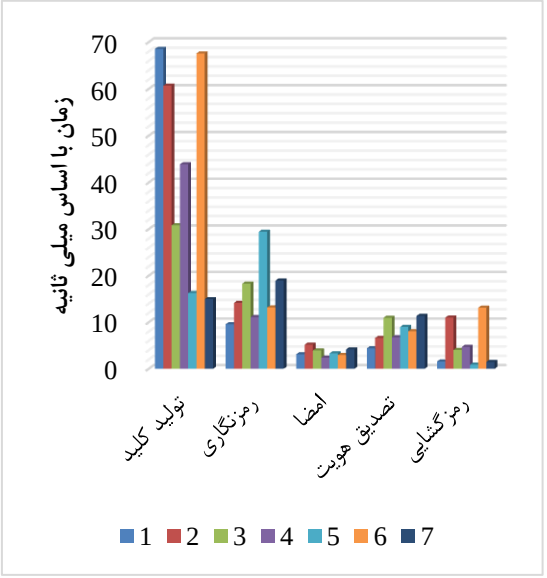
[1] Wi-Fi Direct
[2] End to End
[3] Delay
[4] https://github.com/cossacklabs/themis/wiki/Secure-Message-cryptosystem



(۲) (۱)

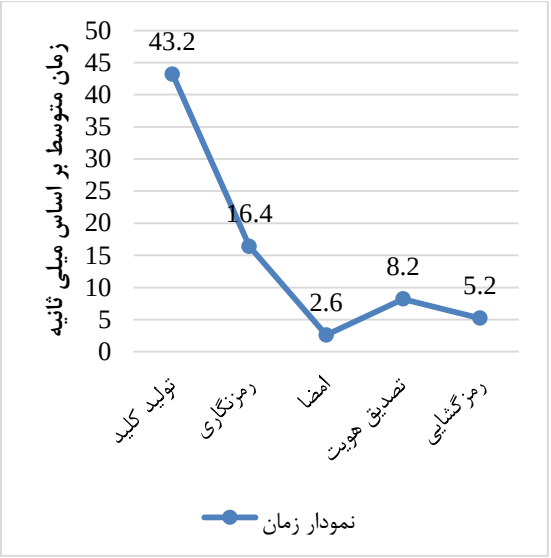
شکل ۹. خروجی برنامه بر روی گوشی؛ (۱) اجرا بر روی گوشی Asus Zenfon3، (۲) اجرا بر روی گوشی Note 5

برنامه بر روی هر یک از گوش‌های هوشمند جدول ۱ یکصد بار اجراشده است. متوسط زمان اجرای موردنیاز برای هرکدام از پنج فرایند تولید کلید، رمزنگاری، امضاء، تصدیق هویت (با بررسی امضاء) و رمزگشایی برحسب میلی‌ثانیه در شکل ۱۰ نشان داده شده است.



شکل ۱۰. نمودار زمانی تولید کلید، رمزنگاری، امضا، تصدیق هویت و رمزگشایی

میانگین زمان اجرای هر کدام از مراحل در شکل ۱۱ نشان داده شده است. همانگونه که مشاهده می‌شود بیشترین زمان بعد از تولید کلید، صرف رمزنگاری اطلاعات شده است.



شکل ۱۱. نمودار متوسط زمانی تولید کلید، رمزنگاری، امضا، تصدیق هویت و رمزگشایی

تعداد بسته‌هایی که گره به گروه می‌فرستد (m) و سرور در جواب برمی‌گرداند (s) یکی از بحث‌های مهم است (ساکای، ۲۰۱۷). زیرا اگر این اعداد برابر یک باشند، امکان آن وجود دارد در این نوع شبکه گره هم‌گروهی گیرنده، به دلایل مختلف از دسترس خارج‌شده و اطلاعات از بین بروند. از طرفی بالا بودن این عدد نیز موجب افزایش ترافیک شبکه، هزینه و مشکلات امنیتی می‌شود (ساکای، ۲۰۱۷). پس لازم است برای آن به‌وسیله مدل ریاضی و تحلیل عددی معیاری مناسب به دست آورد کد که در مقاله (ساکای، ۲۰۱۷) به‌صورت مفصل به بررسی آن پرداخته‌شده است.

۴-۱- مقایسه روش پیشنهادی با روش‌های مطرح‌شده در پژوهش‌های قبلی

در مقاله (ساکای، ۲۰۱۷) به‌منظور انتقال امن داده‌ها در بستر شبکه‌هایی باتحمل تأخیر بالا، سازوکار مسیریابی پوست‌پیازی گروهی مطرح‌شده است. استفاده همین روش برای حل مشکل بیان‌شده در اینترنت اشیاء امکان‌پذیر و امنیت و گمنامی اطلاعات را به‌خوبی برقرار می‌کند. باید توجه داشت، منابع گره‌ها محدود است و با توجه به آنچه در قسمت تحلیل آمده است، فرایند رمزنگاری، امضا، تصدیق هویت و رمزگشایی هزینه زمانی زیادی برای هر گره دارد. مشکل دیگر در استفاده کامل از این روش، گام ورود اطلاعات به شبکهٔ اینترنت است،

زیرا به دلیل محدودیت‌هایی که برخی از شرکت‌های ارائه‌دهنده سرویس اینترنت[1]، بر روی مسیریابی پوست‌پیازی اعمال کرده‌اند (کوخ، ۲۰۱۶)، امکان عدم استفاده از تجهیزات محیط در گام ورود به اینترنت وجود دارد که این امر مانع ارسال سریع اطلاعات به مقاصد دورتر می‌شود (ایشان، ۲۰۲۱).

همچنان در مقاله (کواسییم، ۲۰۱۸) روش‌های مختلفی برای تأمین امنیت اینترنت اشیاء موردبررسی قرارگرفته‌اند که یکی از بهترین روش‌های مطرح‌شده بنا به گفته محقق، استفاده از سازوکار زنجیرهٔ بلوکی است. در این روش، گره‌ها به‌منظور ارسال اطلاعات خود به مقصد از زنجیرهٔ بلوکی استفاده کرده‌اند. استفاده از این روش به‌تنهایی برای حل مشکل بیان‌شده امکان‌پذیر نیست، زیرا سازوکار روش زنجیرهٔ بلوکی نیازمند دسترسی مستقیم به کاوشگرها، به‌منظور استفاده از منابع پردازشی آن‌ها، و درنتیجه ارتباط مستقیم با اینترنت است. از طرفی دیگر باوجود قابل‌اطمینان بودن روش زنجیرهٔ بلوکی و تأمین اکثر موارد امنیتی توسط سازوکار آن، روش تأمین گمنامی در آن با استفاده از نام مستعار بوده که امکان نقض گمنامی در آن وجود دارد (موزر، ۲۰۱۳).

در روش پیشنهادی، به دلیل استفاده از یک گام رمزنگاری، سربار زمانی رمزنگاری موجود در مقاله (ساکای، ۲۰۱۷) از تعداد گام‌های مابین مبدأ و مقصد به یک مرحله کاهش پیدا می‌کند. از طرفی چون در گام اتصال به اینترنت از سازوکار مسیریابی پوست‌پیازی استفاده نشده، درنتیجه استفاده از زیرساخت‌های موجود در محیط با محدودیت مواجه نمی‌شود. از طرفی در گام ارسال اطلاعات به اینترنت از سازوکار زنجیرهٔ بلوکی با بهبودهای معرفی‌شده در (موزر، ۲۰۱۳) استفاده‌شده با روش کیف پول اشتراکی، ضمن بهره‌مند شدن از مزایای زنجیرهٔ بلوکی، مشکل ایجاد گمنامی کامل برای گروه نیز حل شود. مطالب بیان‌شده در این بخش به‌طور مختصر در جدول ۲ بیان‌شده است.

جدول ۲. مقایسه روش پیشنهادی با روش‌های قبل

روش / مشخصه	مسیریابی پوست‌پیازی	زنجیرهٔ بلوکی	روش پیشنهادی
امنیت بالا	✓	✓	✓
گمنامی کامل	✓	x	✓
پردازش کم در گره‌ها	x	✓	✓
به‌کارگیری زیرساخت‌های موجود	x	✓	✓

[1] ISP

استفاده مستقیم در DTN	✓	×	✓

نتیجه‌گیری

با توجه به تحلیل‌های انجام‌شده و مطالعات حاصل از پژوهش‌های پیشین، گام رمزنگاری یکی از مراحل زمان‌بر است که استفاده از آن در دستگاه‌هایی با توان پردازشی و منابع محدود، کار مقرون به‌صرفه‌ای نیست (کواسییم، ۲۰۱۸). همچنان باید توجه داشت که ممکن است به دلایلی گره ارتباط مستقیم با اینترنت نداشته باشد که نتیجه‌ی آن در دسترس نبودن آن خواهد بود. درنتیجه باید از سازوکار شبکه‌ها باتحمل تأخیر استفاده کرد تا امکان در دسترس بودن گره افزایش یابد. از طرف دیگر بسیاری از کشورها استفاده از سازوکار سیستم‌های مسیریابی پوست‌پیازی را در داخل شبکه‌های خود ممنوع و راه‌های آن را محدود کرده‌اند (کوخ، ۲۰۱۶). درنتیجه استفاده از روش پیشنهادی در (ساکای، ۲۰۱۷) در این کاربرد، باعث افزایش گام پردازشی گره‌ها و کاهش احتمال امکان استفاده از زیرساخت‌های موجود در محیط می‌شود. به‌منظور کاهش بار پردازشی، درروش پیشنهادی این کار تنها یک‌بار و توسط گره مبدأ انجام می‌شود. به‌منظور تأمین امنیت اطلاعات در استفاده از زیرساخت‌های محیط، در گام ارسال اطلاعات به اینترنت، از سازوکار سیستم‌های زنجیرهٔ بلوکی با استفاده از روش‌های سرویس‌های ترکیب‌کننده و کیف پول اشتراکی استفاده می‌شود.

به‌این‌ترتیب، اتصالی امن بین گره‌های موجود در محیط ایجاد می‌شود که هر گره بین $k-1$ عضو دیگر گروه از دید اعضای دیگر گمنام می‌گردد، زیرا حتی گره‌هایی که بسته را انتقال می‌دهند، اطلاع ندارند که بسته را از مولد آن به‌صورت مستقیم دریافت کرده‌اند یا از طریق گره‌های واسط بسته به آن‌ها رسیده است. از طرف دیگر، در خارج از گروه نیز با توجه به سازوکار شبکه زنجیرهٔ بلوکی، گمنامی خود گروه به‌صورت کامل برقرار می‌شود.

روش پیشنهادی در این پژوهش می‌تواند برای حفظ گمنامی و حریم خصوصی کاربران، تجهیزات و دستگاه‌های متصل به شبکه‌های اینترنت اشیاء در هنگام تبادل اطلاعات و داده‌های جمع‌آوری شده توسط آن‌ها استفاده گردد.

منابع

Conoscenti, M.; Antonio, V.; & Juan C., De, M.. (2016). Blockchain for the Internet of Things: A systematic literature review. *13th International Conference of Computer Systems and Applications (AICCSA)*. 2016.

Faris, E., Hosseini, Mohammad, R., Matarneh, S., Talebi, S., Igor M., Song W., Poshdar, M., & Ghodrati, N. (2021). Blockchain and the Internet of Things for the construction industry: research trends and opportunities. *Automation in construction. Vol.* 132, pp. 103-111.

Ishan, K., Ahmed, N., Malaney, R., Rafiqul, I., & Jha, S. (2021). De-anonymisation attacks on Tor: A Survey. *IEEE Communications Surveys & Tutorials, Vol.* 23, No. 4, pp. 2324-2350.

Joshi, A. P., Meng, H., & Yan, W. (2018). A survey on security and privacy issues of blockchain technology. *Mathematical foundations of computing*. Vol. 1, No.2, 2018, pp. 121-147.

Jung, W.-S., Hyochun, A., & Young-Bae, K. (2014), Designing content-centric multi-hop networking over Wi-Fi Direct on smartphones. *IEEE Wireless Communications and Networking Conference (WCNC)*. 2014.

Koch, R.; Mario, G., & Gabidreo, R. (2016). How anonymous is the tor network? A long-term black-box investigation. *Computer Networks*. Vol. 49, No. 3, 2016, pp. 42-49.

Kouicem, D.; Eddine, A.; & Hicham, L. (2018). Internet of things security: A top-down survey. *Computer Networks*. Vol. 141, No 1, 2018, pp. 199-221.

Lin, I-C.; & Tzu-Chun, L. (2017). A survey of blockchain security issues and challenges. (2017). *Inteligence Journal Network Security*. Vol. 19, No. 5, 2017, pp. 653-659.

Miller, D. (2018). Blockchain and the internet of things in the industrial sector. *IT professional, Vol.* 20, No. 3, pp. 15-18.

Moser, Malte. (2013), Anonymity of bitcoin transactions. (2013).

Moubarak, J.; Eric, F.; & Maroun, C. (2017). Comparative analysis of blockchain technologies and tor network: Two faces of the same reality?.. *1st Cyber Security in Networking Conference (CSNet)*.

Ojha, G.; Rakesh, S.; & Anupam, S. (2016). Improved Identity Anonymization Using Hashed-TOR Network. *Artificial Intelligence and Evolutionary Computations in Engineering Systems*. pp. 185-192.

Romi, K.; Terjesen, S.; & Liu, C. (2021). Blockchain, Bitcoin, and ICOs: a review and research agenda. *Small Business Economics, Vol* 56, No. 4, pp. 1699-1720.

Sakai, K. (2017). Performance and security analyses of onion-based anonymous routing for delay tolerant networks. *IEEE Transactions on Mobile Computing.* Vol. 16, No.12, 2017, pp. 3473-3487.

Sun, Y.; Lei Z., Gang F.; Bowen Y., Bin C.; & Imran, Muhammad Ali. (2019). Blockchain-enabled wireless Internet of Things: Performance analysis and optimal communication node deployment. *IEEE Internet of Things Journal,* Vol. 6, No. 3, pp. 5791-5802.

Wang, J.; & Li, M. (2018). A blockchain based privacy-preserving incentive mechanism in crowdsensing applications. *IEEE Access*, Vol. 6, No 2, 2018, pp. 17545-17556.

Zhao, C.; & Yang, S. (2016). Rapid, user-transparent, and trustworthy device pairing for d2d-enabled mobile crowdsourcing. *IEEE Transactions on Mobile Computing*, Vol. 16, No. 7, 2016, pp. 2008-2022.