Karafan

Quarterly Scientific Journal of National University of Skill

Winter 2025, Vol. 21, No. 4, p. 307-336

Journal Homepage: https://karafan.nus.ac.ir/?lang=en

doi:10.48301/KSSA.2024.476579.2982

Hardware-software Cyber Security Platform for Data Protection in Smart Agricultural Wireless Sensor Network with Signal Processing Capability

Abdolah Safari Dehnavi[1*], Vahid Safari Dehnavi[2]

[1]Department of Agriculture Engineering, National University of Skills (NUS), Tehran, Iran.
[2]Department of Electrical Engineering, Amirkabir University of Technology, Tehran, Iran/ Department of Electrical Engineering, National University of Skills (NUS), Tehran, Iran.

ARTICLE INFO

Article Type:
Original Research

Received: 09.12.2024
Revised: 10.19.2024
Accepted: 11.24.2024

Keyword:
Wireless Sensor Networks
Smart Agriculture
Hardware
Security Protocol
Fault Detection

***Corresponding Author:**
Abdolah Safari Dehnavi
Email: *asafari@tvu.ac.ir*

ABSTRACT

With the increase in population and the growth of demand for agricultural products, it is necessary to use new technologies to increase productivity. Wireless sensor networks, as one of the key technologies in smart agriculture, enable continuous and accurate monitoring of environmental parameters such as temperature and humidity. These systems provide farmers with the possibility of optimal management of resources by wirelessly transmitting information to control centers. This technology faces important challenges, such as information security and efficiency in heterogeneous and distributed environments. Reviewing the previous research found that the existing articles have not comprehensively addressed the security and efficiency of these systems. Therefore, this paper aims to provide a comprehensive solution to improve the efficiency of wireless sensor networks in smart agriculture. Also, appropriate hardware for accurate monitoring of environmental parameters, including temperature and humidity sensors, has been introduced and implemented. To improve the accuracy of data processing and control, the optimized convolutional neural network with a genetic algorithm was used for fault detection, and the proposed control algorithm was used to control the speed of agricultural motors. The proposed security protocol was formally and informally evaluated using the Scyther tool. The results showed a significant improvement in information security and reduced energy consumption. Also, by using vibration data, we achieved 99.92% accuracy for test data, and by simultaneously using vibration and acoustic data, we achieved 99.96% test accuracy, indicating the data combination's effectiveness for fault detection. In addition, the control algorithm could control the motor speed well in fault-free and faulty modes.

©2025 the authors. Published by National University of Skill, Tehran, Iran. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution-Noncommercial 4.0 International (CC BY-NC License) (https://creativecommons.org/licenses/by-nc/4.0/)

E-ISSN: 2538-4430
ISSN: 2382-9796

EXTENDED ABSTRACT

Introduction

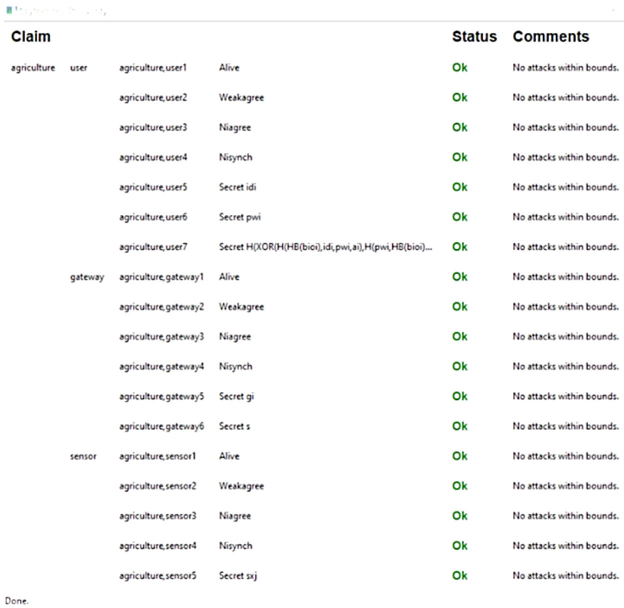
The world is seriously facing an increase in population and a rising demand for agricultural products. In developed countries, wireless sensor network technology is among the emerging technologies used for sensing agricultural environments, collecting information, and transmitting it to the user or a central station for proper monitoring and response. In recent years, wireless sensor networks have significantly contributed to smart agriculture's growth and increased productivity in agricultural and greenhouse environments.

Methodology

This paper presents a structure that includes the design of a cybersecurity protocol, hardware proposals, and an algorithm for status monitoring and control. After reviewing the studies conducted on wireless sensor networks in agricultural environments, we concluded that the existing research has not been able to consider all security aspects and the efficiency of this technology. Therefore, in this study, we proposed a design to improve the performance of wireless sensor networks deployed in agricultural environments. We also verified our proposed design informally and formally using the Scyther tool. Subsequently, suitable hardware, an improved convolutional neural network, and a control algorithm are proposed to transmit temperature and humidity data, detect faults, and intelligently control the motors used in agriculture. The results indicate that the proposed design is suitable for security, monitoring algorithms, and control efficiency, and it provides the necessary performance for deployment in smart agricultural environments.

Results and discussion

Designed protocol: In the proposed design, no symmetric or asymmetric encryption and heavy-weight operators such as scalar multiplication or exponentiation are used, and only the hash function and XOR operator are used, which do not require much overhead in calculations and time. On the other hand, each Hash will take about 0.0004 milliseconds, each scalar multiplication will take 7.3529 milliseconds, and each symmetric encryption will take 0.1303 milliseconds, and since the proposed scheme only Hash used will have a perfect execution time compared to other schemes that used cryptography and other heavy-weight operators such as scalar multiplication. The output of the Scyther tool is shown if Figure 1.



Claim				Status	Comments
agriculture	user	agriculture,user1	Alive	Ok	No attacks within bounds.
		agriculture,user2	Weakagree	Ok	No attacks within bounds.
		agriculture,user3	Niagree	Ok	No attacks within bounds.
		agriculture,user4	Nisynch	Ok	No attacks within bounds.
		agriculture,user5	Secret idi	Ok	No attacks within bounds.
		agriculture,user6	Secret pwi	Ok	No attacks within bounds.
		agriculture,user7	Secret H(XOR(H(HB(bioi),idi,pwi,ai),H(pwi,HB(bioi)...	Ok	No attacks within bounds.
	gateway	agriculture,gateway1	Alive	Ok	No attacks within bounds.
		agriculture,gateway2	Weakagree	Ok	No attacks within bounds.
		agriculture,gateway3	Niagree	Ok	No attacks within bounds.
		agriculture,gateway4	Nisynch	Ok	No attacks within bounds.
		agriculture,gateway5	Secret gi	Ok	No attacks within bounds.
		agriculture,gateway6	Secret s	Ok	No attacks within bounds.
	sensor	agriculture,sensor1	Alive	Ok	No attacks within bounds.
		agriculture,sensor2	Weakagree	Ok	No attacks within bounds.
		agriculture,sensor3	Niagree	Ok	No attacks within bounds.
		agriculture,sensor4	Nisynch	Ok	No attacks within bounds.
		agriculture,sensor5	Secret sxj	Ok	No attacks within bounds.

Done.

Figure 1. Output of the Scyther tool for the proposed design.

Signal processing and fault diagnosis algorithm: This section presents the accuracy of the fault diagnosis algorithm and the motor speed controller. In order to train the network, 21503 data were used, 2688 data were used for validation, and 2688 data were used for testing. The results are shown in Table 1 and Figure 2- Figure 4. In Table 1, A1 represents the first vibration sensor, A2 the second vibration sensor, A3 the third vibration sensor, and ACO the acoustic sensor. As can be seen in Table 1, in the case where a combination of sensors is used, the fault detection accuracy is higher. In addition, in the case where the combination of acoustic and vibration sensors is used, compared to the case where only vibration sensors are used, the accuracy of fault detection is higher. In this article, a PID controller is used to control the speed of the motor. The simulation method assumes that the motor is healthy from the moment of starting up to 3 seconds. In this second, a fault occurs, and time is required for the fault detection process. After detecting the fault, the supplementary controller enters the control algorithm that leads to speed control after the fault occurs. The control method presented in this article was able to effectively control the speed, and this control happened with the most negligible impact on the torque and stator currents.

Table 1. Data classification results.

Sensors	Train accuracy	Validation accuracy	Test accuracy	Train time (sec)	Number of parameters
A1 [4]	85.21	84.76	84.64	30	-
A1 [26]	61.44	62.20	62.61	379	42504
A1	100	99.93	99.92	2735	105832
A2	98.54	97.32	97.22	2716	105832
A3	98.60	97.14	97.76	2760	105832
ACO	95.85	94.90	94.97	2694	105832

Sensors	Train accuracy	Validation accuracy	Test accuracy	Train time (sec)	Number of parameters
A1, A2, A3 [26]	71.78	71.98	71.13	772	105992
A1, A2, A3	99.89	99.85	99.88	5968	247912
A1, A2, ACO	99.31	99.70	99.77	6335	247912
A1, A3, ACO	99.93	100	99.96	6285	247912

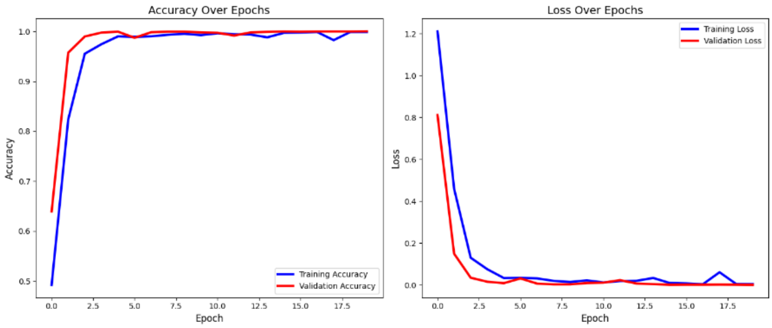


Figure 2. Classification results for combination of vibration and acoustic sensors.

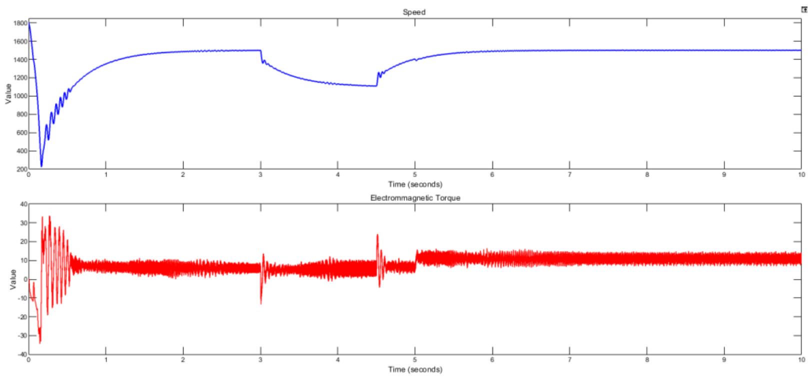


Figure 3. Motor speed and torque before and after the fault.

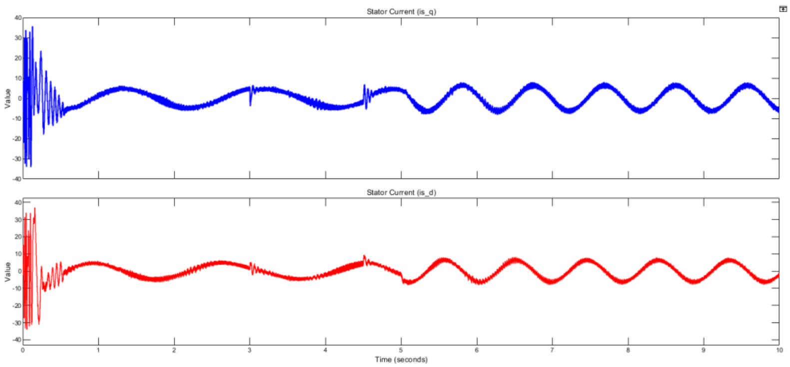


Figure 4. d-q axis stator current before and after the fault occurs.

Conclusion

This paper aimed to present a safe hardware-software proposal for wireless sensor networks deployed in agricultural land and smart greenhouse environments, which can consider all security aspects and does not add too much overhead to the system. For this reason, we presented an authentication and key agreement protocol for wireless networks deployed in agricultural land that uses lightweight operators. We further proved that the proposed scheme not only meets the security requirements but is also resistant to possible attacks by attackers. It does not add much overhead to the network and is suitable for practical implementation in agricultural environments facing energy constraints. Then, two hardwares were proposed to collect low-frequency and high-frequency environmental data with two data transmission protocols. After that, to intelligentize the condition monitoring process, a deep neural network was used to classify defects and control the engine speed of agricultural pumps and irrigation systems. In this case, it was shown that the proposed method and the combined use of vibration and acoustic sensors had good results. Also, the controller was able to control the speed of the engine in a healthy state and a faulty state.

کارافن
فصلنامه علمی دانشگاه ملی مهارت
زمستان ۱٤۰۳، دوره ۲۱، شماره ٤، ۳۳٦-۳۰۷
آدرس نشریه: https://karafan.nus.ac.ir/
doi: 10.48301/KSSA.2024.476579.2982

زیرساخت سخت‌افزاری- نرم‌افزاری امنیت سایبری برای حفاظت داده‌ها در شبکه حسگری بی‌سیم کشاورزی هوشمند با قابلیت پردازش سیگنال

عبداله صفری دهنوی[۱*]، وحید صفری دهنوی[۲]

۱- عضو هیات علمی، گروه مهندسی کشاورزی، دانشگاه ملی مهارت، تهران، ایران.

۲- گروه مهندسی برق کنترل، دانشگاه صنعتی امیرکبیر، تهران، ایران/ مدرس، گروه مهندسی برق، دانشگاه ملی مهارت، تهران، ایران.

اطلاعات مقاله

نوع مقاله: مقاله پژوهشی

دریافت مقاله: ۱۴۰۳/۰۶/۲۲
بازنگری مقاله: ۱۴۰۳/۰۷/۲۸
پذیرش مقاله: ۱۴۰۳/۰۹/۰۴

کلید واژگان:
شبکه‌های حسگر بی‌سیم
کشاورزی هوشمند
سخت‌افزار
پروتکل امنیتی
تشخیص عیب

***نویسنده مسئول:** عبداله صفری دهنوی
پست الکترونیکی:
asafari@tvu.ac.ir

چکیده

با افزایش جمعیت و رشد تقاضا برای محصولات کشاورزی، بهره‌گیری از فناوری‌های نوین برای افزایش بهره‌وری ضروری هست. شبکه‌های حسگر بی‌سیم، به عنوان یکی از فناوری‌های کلیدی در کشاورزی هوشمند، امکان پایش مستمر و دقیق پارامترهای محیطی نظیر دما و رطوبت را فراهم می‌کنند. این سیستم‌ها با انتقال بی‌سیم اطلاعات به مراکز کنترل، امکان مدیریت بهینه منابع را در اختیار کشاورزان قرار می‌دهد. این فناوری با معضلات مهمی نظیر امنیت اطلاعات و کارایی در محیط‌های ناهمگن و پراکنده مواجه است. با مرور تحقیقات پیشین مشخص شد که مقالات موجود به‌صورت جامع به امنیت و کارایی این سیستم‌ها نپرداخته‌اند. بنابراین، هدف این مقاله، ارائه یک راهکار جامع برای بهبود کارایی شبکه‌های حسگر بی‌سیم در کشاورزی هوشمند است. همچنین، سخت‌افزارهای مناسب برای پایش دقیق پارامترهای محیطی، از جمله حسگرهای دما و رطوبت، معرفی و اجرا شده است. به‌منظور بهبود دقت پردازش داده و کنترل، از شبکه عصبی کانولوشنی بهینه‌شده با الگوریتم ژنتیک برای تشخیص عیب و از الگوریتم کنترلی پیشنهادی برای کنترل سرعت موتورهای کشاورزی استفاده شد. پروتکل امنیتی پیشنهادی به صورت رسمی و غیررسمی با استفاده از ابزار اسکایتر ارزیابی شد. نتایج نشان‌دهنده بهبود قابل‌توجهی در امنیت اطلاعات و کاهش مصرف انرژی بود. همچنین با استفاده از داده‌های آزمایش ارتعاش به دقت ۹۹.۹۲ درصد و با استفاده همزمان از داده‌های ارتعاش و آکوستیک به دقت ۹۹.۹۶ درصد دست یافتیم که بیانگر مؤثربودن ترکیب داده‌ها برای تشخیص عیب است. همچنین الگوریتم کنترلی به‌خوبی توانست سرعت موتور را در حالت بدون عیب و با عیب کنترل کند.

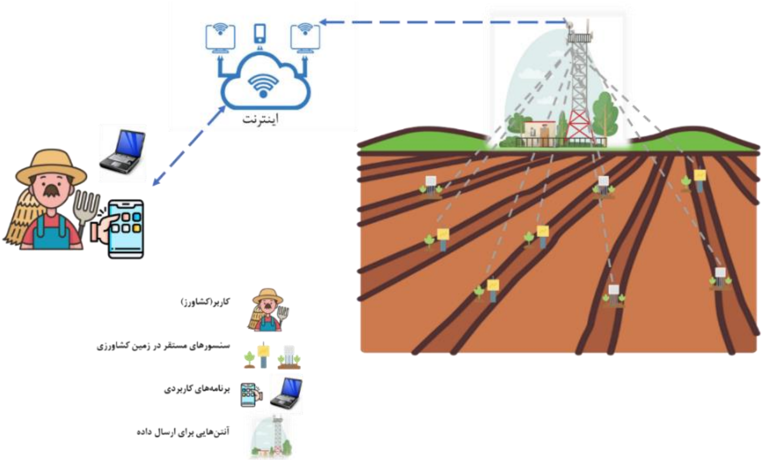
شاپای الکترونیکی: ۲۵۳۸-۴۴۳۰
شاپای چاپی: ۲۳۸۲-۹۷۹۶

©2025 the authors. Published by National University of Skill, Tehran, Iran. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution-Noncommercial 4.0 International (CC BY-NC License) (https://creativecommons.org/licenses/by-nc/4.0/)

مقدمه

با توجه به اعلام سازمان غذا و کشاورزی ملل متحد (فائو) پیش‌بینی می‌شود که تا سال ۲۰۵۰ میلادی جمعیت جهان به ۹.۶ میلیارد نفر برسد و به طبع تقاضا برای مواد غذایی ۷۰ درصد افزایش می‌یابد. افزایش جمعیت جامعه جهانی و همچنین افزایش تقاضا برای محصولات کشاورزی باعث خواهد شد که نیاز به نوسازی روش‌های کشاورزی و بهره‌برداری از زمین‌های کشاورزی به‌طور ویژه حس شود [۱]. در دهه‌های گذشته، کشاورزی شاهد تغییر و تحولات بسیاری در حوزه صنعتی‌شدن و مدیریت مبتنی بر فناوری بوده است. با استفاده از کشاورزی هوشمند و فناوری‌های جدید، این امکان برای کشاورزان ایجاد شده است که کنترل بهتری در روند کشت، برداشت و مراقبت از محصولات زراعی داشته باشند.

امروزه پیشرفت و گسترش اینترنت در بخش‌های مختلف زندگی بشر بر کسی پوشیده نیست. ظهور و پیشرفت فناوری‌های جدید مانند شبکه‌های حسگر بی‌سیم[1] در همه جنبه‌های زندگی بشر، از جمله حمل‌ونقل، اتوماسیون منازل و پزشکی از راه دور را تحت تأثیر قرار داده است. طبیعتاً حوزه کشاورزی نیز از این قاعده مستثنا نیست. از اینترنت اشیا[2] و شبکه‌های حسگر بی‌سیم می‌توان به عنوان فناوری‌های نوظهوری یاد کرد که می‌توان از آن‌ها در راستای پیشرفت صنعت کشاورزی و هوشمندتر شدن کشاورزی از آن‌ها بهره برد [۲]. برای مثال می‌توان از سنسورهای نظارت بر خاک، سنسورهای نظارت بر آب و هوا یا سنسورهای کنترل‌کننده آب‌پاش و نور برای بهبود فرایند پایش و کنترل فرایند کشاورزی یا محیط‌های گلخانه‌ای بهره برد. نمونه‌ای از سناریو استفاده از شبکه‌های حسگر بی‌سیم در بسترهای کشاورزی در شکل ۱ قابل مشاهده است. در این سناریو کشاورز قادر خواهد بود از طریق برنامه‌های کاربردی که بر روی تلفن همراه خود نصب دارد، سنسورهایی که در زمین‌های کشاورزی وجود دارند را بررسی کند و در صورت لزوم دستوری را ارسال کند.



شکل ۱. سناریو استفاده از شبکه‌های حسگر بی‌سیم در بسترهای کشاورزی.

همان‌طور که بیان شد استفاده از فناوری شبکه‌های حسگر بی‌سیم مزایای بسیاری برای محیط‌های کشاورزی و گلخانه‌ای دارد، با این وجود به دلیل استفاده از اینترنت که بستری ناامن است در صورت وجود خرابی یا عملکرد اشتباه، احتمال آسیب‌های جبران‌ناپذیری وجود دارد. برای مثال حالتی را درنظر بگیرید که سنسورهایی در محیط گلخانه‌ای

---

[1] Wireless Sensor Network (WSN)
[2] Internet of Things

برای کنترل دما قرار داده شده‌اند که دمای محیط گلخانه را اندازه می‌گیرند و از طریق اینترنت برای کشاورز ارسال می‌کند. حال در صورتی که این پیام در راه دستکاری شود و به هر علتی به‌درستی به دست کشاورز نرسد ممکن است باعث خرابی یا حتی فاجعه‌ای در حد آتش‌سوزی شود و کشاورز با توجه به اعتماد به هوشمندبودن گلخانه از این موضوع بی‌اطلاع بماند. برای مثالی دیگر می‌توان حالتی را درنظر گرفت که با توجه به هوشمندبودن محیط کشاورزی، کاربر مربوطه فرمان آبپاشی به میزان مشخصی را در زمان مشخص از طریق اپلیکیشنی که در اختیار دارد بر روی بستر اینترنت و از راه دور ارسال کند. این امکان وجود دارد که مهاجمین، پیام کاربر مربوطه را دستکاری کنند و پیام به صورت صحیح توسط سنسورها دریافت نشود و باعث خرابی محصولات کشاورزی خواهد شد.

در همین راستا پژوهشگران بسیاری برای بهبود وضعیت شبکه‌های حسگر بی‌سیم مستقر در بستر کشاورزی و گلخانه‌ای طرح‌هایی را ارائه داده‌اند [۳-۸]. در این پژوهش پس از بررسی طرح‌های موجود به این نتیجه رسیدیم که طرح‌های ارائه‌شده توسط پژوهشگران تمامی جنبه‌های امنیتی لازم را درنظر نگرفته‌اند یا سربار زیادی به شبکه حسگر بی‌سیم وارد می‌کنند؛ به‌طوری که کارایی لازم را ندارند. به همین دلیل در این پژوهش هدف ما این است که طرحی در قالب یک پروتکل برای شبکه‌های حسگر بی‌سیم برای بسترهای کشاورزی هوشمند ارائه دهیم که علاوه بر درنظرگرفتن کارایی لازم، جنبه‌های امنیتی محرمانگی و صحت داده‌های تبادل‌شده بین موجودیت‌های درگیر در این بستر را درنظر بگیرد.

در ادامه به‌طور کامل مرور خواهیم کرد که پژوهشگران چه طرح‌هایی را برای شبکه حسگری بی‌سیم ارائه دادند و طرح‌های آن‌ها چه ویژگی‌هایی دارد. در ادامه به طرح پیشنهادی خود خواهیم پرداخت و ویژگی‌های آن را برای بسترهای کشاورزی بیان خواهیم کرد. در انتها نیز به اثبات امنیت و کارایی طرح پیشنهادی می‌پردازیم و نشان می‌دهیم که طرح پیشنهادی در مقایسه با سایر طرح‌ها عملکرد بهتری خواهد داشت. به‌منظور اثبات امنیت طرح پیشنهادی در بخش بحث و نتایج، از اثبات رسمی با نرم‌افزار اسکایتر و روش غیررسمی استفاده می‌شود. شیوه اثبات بدین صورت است که امنیت و کارایی پروتکل در مقابل نفوذ، مهاجم‌ها و حملات سایبری بررسی می‌شود. نرم‌افزار اسکایتر شرایط و درگاه‌های نفوذ مختلف را بررسی می‌کند و در صورتی که مشکل امنیتی نباشد، تأییدیه می‌دهد. همچنین این پروتکل، یک پروتکل بسیار سبک‌وزن است که برای سنسورهای مورداستفاده در شبکه حسگری بی‌سیم که توان و انرژی پردازشی کمی دارند، مناسب است. در زیربخش تحلیل کارایی طرح پیشنهادی در جدول ۴، زمان پردازشی این پروتکل با پروتکل‌های مشابه مقایسه شده است. در نهایت الگوریتم کنترلی و پردازش سیگنال ارائه می‌شود، در بخشی از این الگوریتم از داده‌های سهری و دیموند و مدل اَسلم استفاده شده است.

پژوهش‌های پیشین

در ادامه به بررسی پژوهش‌های انجام‌شده‌ای خواهیم پرداخت که پروتکل‌هایی برای شبکه‌های حسگر بی‌سیم ارائه داده‌اند. از طرفی با توجه به این موضوع که سنسورهایی که در شبکه حسگر بی‌سیم در بستر کشاورزی و گلخانه‌ای قرار دارند، دارای انرژی محدودی از نظر باتری، پردازش و حافظه هستند باید به این موضوع توجه شود که طرح ارائه‌شده به چه میزانی کارایی دارد. به همین منظور در جدول ۱ طرح‌های ارائه‌شده به همراه ویژگی‌ها، نقاط ضعف و قوت و میزان کارآمدبودن آورده شده است.

ضرورت طرح پیشنهادی

همان‌طور که بیان شد با رشد جمعیت جهان و افزایش تقاضا در مورد محصولات کشاورزی نیاز به هوشمندسازی سیستم کشاورزی بیش از پیش حس می‌شود. با وجود تمامی مزایایی که استفاده از شبکه‌های بی‌سیم در بستر گلخانه‌ای و هوشمندشدن کشاورزی دارد، ناامن‌بودن بستر اینترنت ممکن است مشکلاتی را برای کشاورزان و

زمین‌های کشاورزی به همراه داشته باشد. پژوهش‌های انجام‌شده در راستای پروتکل‌های شبکه‌های حسگر بی‌سیم نتوانسته‌اند تمامی جنبه‌های لازم برای این بستر را درنظر بگیرند و همچنین کارایی لازم را ندارند به همین دلیل در این پژوهش ما به ارائه ساختاری سخت‌افزاری- نرم‌افزاری نوین برای شبکه‌های حسگر بی‌سیم مستقر در بسترهای کشاورزی و گلخانه‌ای خواهیم پرداخت.

جدول ۱. مروری بر پژوهش‌های پیشین.

طرح‌ها	توضیحات	نقاط ضعف
داس[1] و همکاران [۹]	ارائه یک چارچوب مدیریت کلید کاربر راه دور در شبکه‌های حسگر بی‌سیم	- به‌روزرسانی ناکارآمد رمز عبور [۱۰] - امکان حمله جعل هویت[2] [۱۱] - مستعد حمله داخلی[3] [۱۱]
وادیا[4] و همکاران [۱۲]	طراحی یک طرح احراز هویت برای شبکه‌های حسگر بی‌سیم برای ارتباط امن موجودیت‌ها	- مستعد حمله حدس رمز عبور - دارای سربار زیاد واردشده به سیستم
ترکانویچ[5] و همکاران [۱۳]	طراحی طرحی برای احراز اصالت دوطرفه موجودیت‌هایی که در شبکه حسگر بی‌سیم وجود دارند با استفاده از رمزنگاری‌های سبک‌وزن	اثبات شده است که طرح ترکانویچ در برابر حمله جعل هویت سنسورها مقاوم نیست و به این ترتیب صحت داده‌های جمع‌آوری‌شده از بسترهای کشاورزی نمی‌تواند مورداعتماد باشد [۱۴]
سونی[6] و همکاران [۱۵]	ارائه یک طرح سه فاکتوره احرازهویت مبتنی بر رمزنگاری منحنی بیضوی برای بستر شبکه‌های حسگر بی‌سیم که هدف آن نظارت می‌باشد.	- تأمین‌نشدن نیاز امنیتی محرمانگی رو به جلو - سربار بسیار زیاد واردشده به سیستم به دلیل استفاده از رمزنگاری سنگین وزن در طراحی پروتکل
علی[7] و همکاران [۱۶]	طراحی پروتکلی با هدف احراز هویت موجودیت‌های شبکه حسگر بی‌سیم مستقر در محیط‌های کشاورزی	- تأمین‌نشدن نیازهای امنیتی مختلف و صحت اطلاعات - مستعد حمله حدس رمز عبور - مستعد حمله داخلی [۱۷]
فاطیما[8] و همکاران [۱۷]	ارایه طرحی با هدف نظارت و بهبود در ارتباطات بین سنسورهای به‌کار برده‌شده در محیط‌های کشاورزی	- درنظرنگرفتن تمامی نیازهای امنیتی - مستعد حملات شناخته شده مانند جعل هویت - عدم در نظر گرفتن سربار وارده به کانال ارتباطی
الوطیبی[9] و همکاران [۱۸]	ارائه طرحی برای ارتباطات امن در بستر شبکه‌های حسگر بی‌سیم با استفاده از رمزنگاری متقارن	- اشتباه در طراحی پروتکل [۱۹] - نبود مقاومت در برابر حمله جعل هویت - تأمین‌نشدن نیاز امنیتی محرمانگی رو به جلو [۱۹] - نبود مقاومت در برابر دزدیده‌شدن تأییدکننده‌ها [۱۹]
ایتو[10] و همکاران [۵]	در این مقاله یک پروتکل برای ارتباط حسگرها و کاربران در محیط‌های کشاورزی و گلخانه‌ای ارائه	- با توجه به استفاده از رمزنگاری منحنی بیضوی سربار پروتکل طراحی‌شده توسط طراحان بسیار بالا است و این پروتکل برای شبکه‌های حسگر بی‌سیم مناسب نمی‌باشد.

1 Das
2 Impersonation Attack
3 Insider Attack
4 Vaidya
5 Turkanović
6 Soni
7 Ali
8 Fatima
9 Alotaibi
10 Itoo

طرح‌ها	توضیحات	نقاط ضعف
	شد و برای طراحی پروتکل از رمزنگاری منحنی بیضوی استفاده شد.	
چن[1] و همکاران [۲۰]	طراحی پروتکلی برای شبکه‌های حسگر بی‌سیم با هدف نظارت بر بسترهای کشاورزی و گلخانه‌ای	- ناتوان در حفظ محرمانگی داده‌های جمع‌آوری‌شده توسط سنسورها - طراحی پروتکل به‌گونه‌ای است که سربار زیادی را به سیستم وارد می‌کند و طرح پیشنهادی کارآمد نیست.
خالد[2] و همکاران [۲۱]	ارائه طرحی با پشتیبانی از چند گره دروازه برای شبکه‌های حسگر بی‌سیم مستقر در بستر کشاورزی هوشمند	- درنظرنگرفتن نیازهای امنیتی متفاوت - استفاده نکردن از رمزنگاری‌های سبک وزن برای کارآمدترشدن طرح پیشنهادی

روش پیشنهادی

روش پیشنهادی شامل سه زیربخش پروتکل امنیتی، سخت‌افزارهای پیشنهادی به همراه نرم‌افزار فضای ابری و الگوریتم‌های پردازش سیگنال و کنترلی است.

پروتکل امنیتی پیشنهادی

در این بخش با درنظرگرفتن نیازهای لازم در کشاورزی هوشمند و همچنین مشخصه‌های شبکه‌های حسگر بی‌سیم، پروتکلی برای احراز هویت و توافق کلید برای شبکه‌های حسگر بی‌سیم مستقر در بسترهای کشاورزی ارائه خواهیم داد. پروتکل پیشنهادی شامل دو بخش اصلی ثبت‌نام و بخش احراز هویت و توافق کلید می‌باشد. در حقیقت در این پروتکل هدف ما این است که موجودیت‌هایی که در یک شبکه حسگر بی‌سیم حضور دارند مانند سنسورها، آنتن‌های جمع‌آوری داده و همچنین کاربر، قبل از ارسال و تبادل داده برای هم احراز هویت شوند به‌طوری که از این موضوع اطمینان حاصل شود که داده‌های تبادل‌شده در محرمانگی و صحت کامل جابه‌جا می‌شوند و همچنین بعد از مرحله احراز هویت، توافق کلید بین موجودیت‌ها انجام شود به‌طوری که در ادامه ارتباط موجودیت‌ها بتوانند از این کلید توافق‌شده برای تبادل اطلاعات خود استفاده کنند. جدول ۲ نمادهای به‌کاررفته در پروتکل پیشنهادی را به همراه توضیحات نشان خواهد داد و همچنین در ادامه به بیان بخش‌های مختلف پروتکل پیشنهادی خود خواهیم پرداخت.

جدول ۲. نمادهای به‌کاررفته در طرح پیشنهادی.

تعریف	نماد
کشاورز/کاربر i که وظیفه ارسال دستورات را به زیرساخت دارد.	U_i
سنسور j ام که وظیفه ارسال داده به فضای ابری را دارد.	S_j
شناسه کاربر i که برای رمزگذاری فرایند ارسال دستورات به کار می‌رود.	Id_i
رمز عبور کاربر i که برای امنیت بیشتر برای ارسال دستورات درنظر گرفته می‌شود.	PW_{U_i}
کلید محرمانه هر سنسور که برای جلوگیری از دزدیده‌شدن داده‌ها استفاده می‌شود.	sx_j
کلید مخفی گره دروازه یا آنتن‌های مستقر که برای برقراری اتصال امن استفاده می‌شود.	S
کلید جلسه توافق‌شده بین طرفین که برای جلوگیری از ورود افرادی است که مجوز ندارند.	$SK_g = SK_i = SK_j$
شناسه سنسور j ام که به‌منظور ارتباط برای انتقال داده استفاده می‌شود.	Id_i
XOR	$\oplus$

[1] Chen
[2] Khalid

تعریف	نماد
عملیات الحاق	$\|\|$
تابع درهم‌ساز	$h(0)$

مرحله ثبت‌نام کاربر در آنتن‌های تبادل داده یا گره دروازه

در این مرحله فرض بر این است که کاربر یا همان کشاورز برای اینکه بتواند از مزایای شبکه‌های حسگر بی‌سیم استفاده کند، دستگاهی در اختیار او قرار می‌گیرد که قادر است از کارت هوشمند استفاده کند یا درون تلفن همراه او کارت هوشمندی قرار می‌گیرد که می‌تواند از طریق آن با آنتن‌هایی که در محل زمین‌های کشاورزی و سنسورهایی که در زمین کشاورزی قرار گرفته‌اند، ارتباط برقرار کند. در همین راستا کاربر برنامه‌ای را درون تلفن همراه خود نصب می‌کند و برای خود یک شناسه $\mathrm{id_i}$، رمز عبور $\mathrm{pw_{U_i}}$ و یک عدد تصادفی $\mathrm{q_i}$ انتخاب می‌کند. شایان ذکر است که کانال ارتباطی در مرحله ثبت‌نام امن درنظر گرفته شده و در مرحله احراز هویت و توافق کلید کانال ارتباطی کاملاً ناامن فرض شده است.

در ادامه بر اساس رابطه (۱) پارامتر $\mathrm{HId_i}$ را محاسبه می‌کند و پارامترهای $\mathrm{id_i}$ و $\mathrm{HId_i}$ را برای آنتن‌های مستقرشده در زمین کشاورزی ارسال می‌کند. زمانی که پارامترهای ارسالی توسط کاربر برای آنتن‌ها یا گره دروازه دریافت می‌شود، در ابتدا بررسی می‌شود که کاربر دیگری با این شناسه $\mathrm{Id_i}$ ثبت‌نام نکرده باشد. در غیر این صورت زمانی که مشخص شد شناسه ارسالی تکراری نیست، به ازای کاربری که پارامترها را ارسال کرده است، عدد تصادفی $\mathrm{w_i}$ انتخاب می‌شود و سپس بر اساس روابط (۲) تا (۵)، پارامترهایی که در شکل ۲ قابل مشاهده است محاسبه می‌شود و در نهایت پارامترهای $\mathrm{B_i}$ ، $\mathrm{w_i}$ و $\mathrm{C_i}$ را برای کاربر بر روی کانال امن ارسال می‌کند. همچنین به‌ازای هر کاربر درون حافظه گره دروازه پارامترهای $\mathrm{B_i}$ و $\mathrm{w_i}$ نیز ذخیره می‌گردد. در نهایت کاربر پارامتر $\mathrm{q_i}$ را نیز به پارامترهایی که گره دروازه برای او ارسال کرده است، اضافه می‌کند و در نهایت پارامترهای $\mathrm{B_i}$ ، $\mathrm{w_i}$ ، $\mathrm{C_i}$ و $\mathrm{q_i}$ درون حافظه تلفن همراه و یا کارت هوشمندی که درون تلفن همراه قرار دارد، ذخیره می‌شود و مرحله ثبت‌نام کاربر در گره دروازه خاتمه می‌یابد.

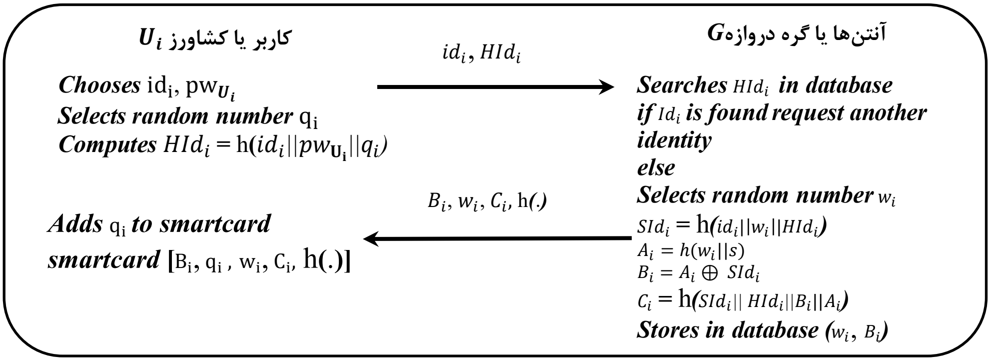
$$HId_i = h(id_i||pw_{\mathbf{U_i}}||q_i) \tag{۱}$$

$$SId_i = h(id_i||w_i||HId_i) \tag{۲}$$

$$A_i = h(w_i||s) \tag{۳}$$

$$B_i = A_i \oplus SId_i \tag{۴}$$

$$C_i = h(SId_i|| HId_i||B_i||A_i) \tag{۵}$$



شکل ۲. مرحله ثبت‌نام کاربر در گره دروازه

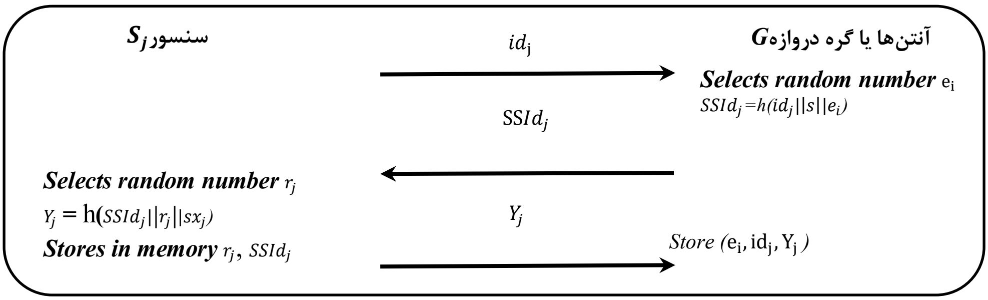
مرحله راه‌اندازی سنسورها

در این مرحله سنسورهای مستقر در زمین‌های کشاورزی و گلخانه‌ای باید راه‌اندازی شود یا به بیان بهتر باید ثبت‌نام شوند. به همین دلیل در ابتدای کار هر سنسور شناسه خود یعنی id_j را برای گره دروازه یا آنتن‌های نصب‌شده در محل ارسال می‌کند. گره دروازه به ازای شناسه هر سنسور عدد تصادفی e_i را انتخاب می‌کند و بر اساس رابطه (۶) پارامتر $SSId_j$ محاسبه می‌شود و در اختیار سنسور بر روی کانال امن قرار می‌گیرد.

$$SSId_j=h(id_j||s||e_i) \tag{۶}$$

در ادامه همان‌طور که در شکل ۳ قابل مشاهده است برای هر سنسور عدد تصادفی r_j انتخاب می‌شود و بر اساس رابطه (۷) پارامتر Y_j محاسبه می‌شود و بعد از ذخیره پارامترهای r_j و $SSId_j$ درون حافظه سنسور پارامتر Y_j نیز در اختیار گره دروازه قرار می‌گیرد و در نهایت پارامترهای Y_j، شناسه هر سنسور یعنی id_j و e_i درون حافظه گره دروازه یا همان آنتن‌های مستقر شده ذخیره می‌شود و مرحله راه‌اندازی سنسور نیز به پایان می‌رسد.

$$Y_j = h(SSId_j||r_j||x_j) \tag{۷}$$



شکل ۳. مرحله راه‌اندازی یا ثبت‌نام سنسورها.

مرحله احراز هویت و توافق کلید

در این مرحله، هدف این است که موجودیت‌های درگیر در پروتکل بعد از اینکه هویتشان برای طرف مقابل اثبات شد یا به اصطلاح احراز هویت دو طرفه صورت گرفت، بر سر یک کلید به توافق برسند و در ادامه راه از این کلید برای ارتباطات خود و تبادل اطلاعات استفاده کنند. در شکل ۴ مراحل احراز هویت و توافق کلید به‌طور کامل قابل مشاهده است.

در مرحله احراز هویت و توافق کلید در ابتدا کاربر باید بتواند به برنامه کاربردی که در اختیار دارد، وارد شود. بدین منظور شناسه خود id_i^* و رمز عبوری $\mathrm{pw}_{\mathbf{U_i}}^*$ که در مرحله ثبت‌نام انتخاب کرده بود را وارد می‌کند. در ادامه همان‌طور که در شکل ۴ قابل مشاهده است، روابط (۸) تا (۱۱) محاسبه می‌شود و سپس پارامتر C_i^* محاسبه‌شده توسط دستگاه موبایل با پارامتر $\mathrm{C_i}$ که درون حافظه تلفن همراه قرار دارد، مقایسه می‌شود. در صورتی که این پارامترها با هم برابر باشند، مشخص می‌شود که کاربر موردنظر همان کاربری است که صاحب تلفن همراه است و مرحله ورود تکمیل می‌شود.

$$HId_i^* = h(id_i^*||pw_{U_i}^*||q_i) \quad (۸)$$

$$SId_i^* = h(id_i^*||w_i||HId_i^*) \quad (۹)$$

$$A_i^* = B_i \oplus SId_i^* \quad (۱۰)$$

$$C_i^* = h(SId_i^*|| HId_i^*||B_i||A_i^*) \quad (۱۱)$$

در ادامه کار موبایلی که در اختیار کاربر قرار دارد، عدد تصادفی $\mathrm{y_i}$ و مهر زمانی $\mathrm{T_1}$ را انتخاب کرده و بر اساس روابط (۱۲) و (۱۳) پارامترهای $\mathrm{U_i}$ و $\mathrm{P_i}$ را محاسبه می‌کند و در نهایت پارامترهای $\mathrm{U_i}$ ، $\mathrm{P_i}$ ،$\mathrm{id_j}$ و مهر زمانی $\mathrm{T_1}$ را برای گره دروازه ارسال می‌کند. در این حالت، فرض بر این است که لیست سنسورهایی که در زمین کشاورزی مستقر هستند، در اختیار کاربر قرار دارد.

$$U_i = h(y_i||T_1||A_i||SId_i\ ) \quad (۱۲)$$

$$P_i = y_i \oplus A_i \quad (۱۳)$$

زمانی که پیام از سمت کاربر به گره دروازه می‌رسد، همان‌طور که در شکل ۴ مشاهده می‌شود گره دروازه در ابتدا تازگی پیام را چک می‌کند در ادامه بر اساس روابط (۱۴) تا (۱۷) پارامترهای $\mathrm{A_i}$، $\mathrm{y_i}$، $\mathrm{SId_i}$ و U_i^* را محاسبه می‌کند و در نهایت با مقایسه پارامترهای U_i^* و $\mathrm{U_i}$ هویت ارسال‌کننده پیام و همچنین صحت پیام ارسالی را بررسی می‌کند.

$$A_i = h(w_i||s) \quad (۱۴)$$

$$y_i = A_i \oplus P_i \quad (۱۵)$$

$$SId_i = A_i \oplus B_i \quad (۱۶)$$

$$U_i^* = h(y_i||T_1||A_i||SId_i) \tag{۱۷}$$

در ادامه عدد تصادفی x_i انتخاب می‌شود و پارامترهای $SSId_j$، F_i، Q_i و G_i بر اساس روابط (۱۸) تا (۲۱) محاسبه و پارامترهای F_i،G_i، id_j و مهر زمانی T_2 برای سنسور ارسال می‌شود.

$$SSId_j = h(id_j||s||e_i) \tag{۱۸}$$

$$F_i = h(SSId_j||id_j) \oplus x_i \tag{۱۹}$$

$$Q_i = y_i \oplus x_i \tag{۲۰}$$

$$G_i = h(x_i \left|\left|Y_j\right|\right| SSId_j||T_2) \tag{۲۱}$$

زمانی که سنسور پیام را از سمت گره دروازه دریافت می‌کند مهر زمانی T_3 را انتخاب می‌کند و با مقایسه آن با مهر زمانی ارسال‌شده مقایسه می‌کند و در صورتی که از تازگی پیام اطمینان حاصل نشود، ارتباط را خاتمه می‌دهد. در غیر این صورت روابط (۲۲) تا (۲۵) محاسبه می‌شود و سپس سنسور کلیدی را بر اساس رابطه (۲۶) محاسبه می‌کند. در انتها پارامتر $Auth_j$ برای اینکه گره دروازه بتواند هر سنسور را احرازهویت کند بر اساس رابطه (۲۷) محاسبه می‌شود و در انتها پارامترهای $Auth_j$ و مهر زمانی T_3 برای گره دروازه و آنتن‌های مستقرشده ارسال می‌شود.

$$SSId_j = h(id_j||s||e_i) \tag{۲۲}$$

$$F_i = h(SSId_j||id_j) \oplus x_i \tag{۲۳}$$

$$Q_i = y_i \oplus x_i \tag{۲۴}$$

$$G_i = h(x_i \left|\left|Y_j\right|\right| SSId_j||T_2) \tag{۲۵}$$

$$SK_j = h(y_i||x_i||Y_j) \tag{۲۶}$$

$$Auth_j = h(SK_j||y_i||T_3||x_i) \tag{۲۷}$$

زمانی که پیام سنسور توسط گره دروازه دریافت می‌شود، پس از بررسی تازگی پیام در ابتدا کلید نشست و پارامتر $Auth_g$ را از روابط (۲۸) و (۲۹) محاسبه می‌کند و در ادامه پارامترهای V_g و M_g را بر اساس روابط (۳۰) و (۳۱) محاسبه می‌کند و این پارامترها را به همراه مهر زمانی T_4 ارسال می‌کند.

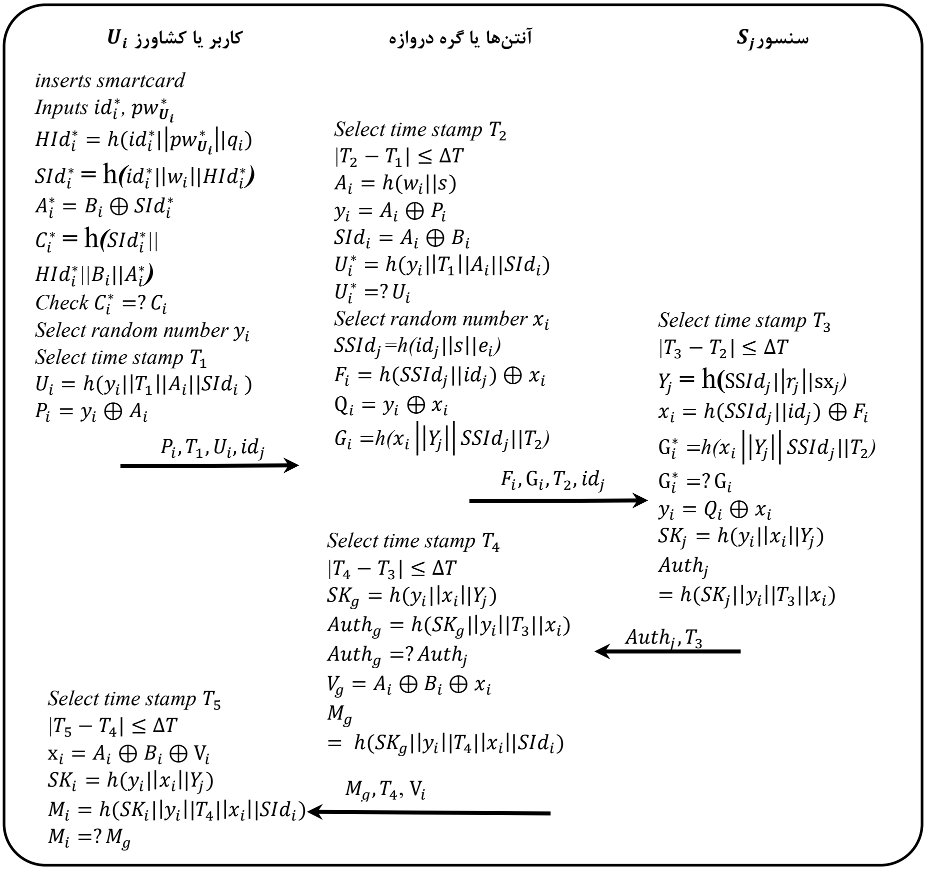
$$SK_g = h(y_i||x_i||Y_j) \tag{۲۸}$$

$$Auth_g = h(SK_g||y_i||T_3||x_i) \quad (۲۹)$$

$$V_g = A_i \oplus B_i \oplus x_i \quad (۳۰)$$

$$M_g = h(SK_g||y_i||T_4||x_i||SId_i) \quad (۳۱)$$

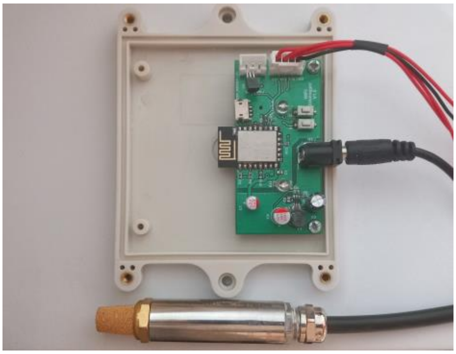
همان‌طور که در شکل ۴ قابل مشاهده است، در انتهای مرحله احرازهویت و توافق کلید، زمانی که پیام گره دروازه توسط تلفن همراه کاربر دریافت می‌شود، در ابتدا تازگی پیام بررسی می‌شود و در صورتی که مشخص شد پیام دریافت‌شده قدیمی و تکراری نیست، کلید جلسه SK_i و پارامتر M_i محاسبه می‌شود و در انتها با مقایسه پارامترهای M_i و M_g ارسال‌کننده پیام احرازهویت می‌شود و همچنین صحت پیام دریافت‌شده نیز تأیید می‌شود و مرحله احرازهویت و توافق کلید پایان می‌یابد.



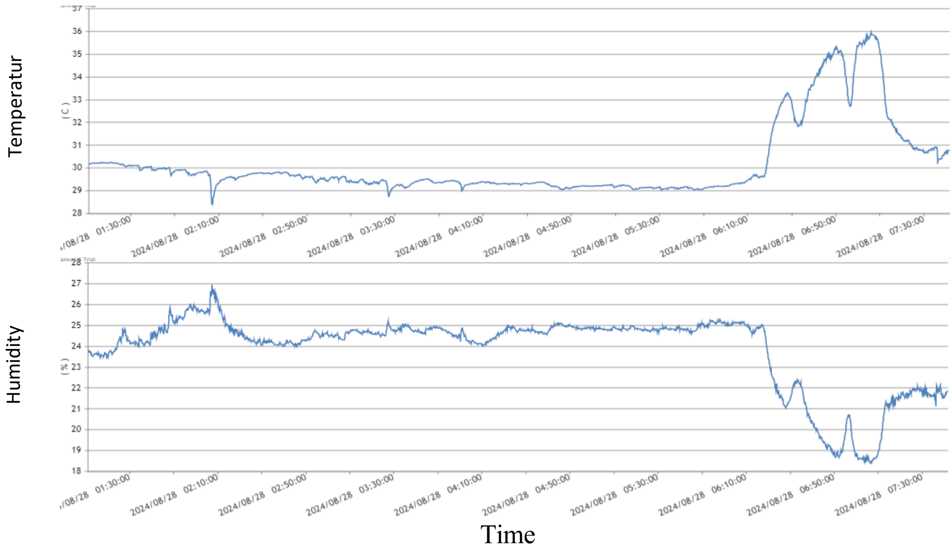
شکل ۴. مرحله احرازهویت و توافق کلید پروتکل پیشنهادی.

سخت‌افزار

در این بخش، سخت‌افزارهای پیشنهادی طراحی‌شده برای ارائه در شبکه حسگری بی‌سیم کشاورزی هوشمند ارائه می‌شود. در این قسمت دو سخت‌افزار ارائه می‌شود، در ابتدا به معرفی دستگاه تله‌متری (سنجش از راه دور) که وظیفه حس کردن و ارسال داده‌های دما و رطوبت روی فضای ابری را دارد و سپس به معرفی دستگاه جمع‌آوری داده فرکانس بالا برای پایش وضعیت موتورهای کشاورزی پرداخته می‌شود. دستگاه اول که وظیفه حس کردن و ارسال داده‌های دما و رطوبت را دارد، در شکل ۵ نشان داده شده است؛ در دستگاه طراحی‌شده، دو سنسور دمایی و یک سنسور رطوبت قرار داده شده است و این اطلاعات به صورت دوره‌ای به فضای ابری منتقل می‌شوند. همچنین برد طراحی‌شده قابلیت توسعه و خواندن اطلاعات ۹ سنسور دما را دارد. نرخ ارسال داده توسط دستگاه به فضای ابری در سایت تعبیه شده است و از طریق موبایل یا کامپیوتر قابل تنظیم است. در شکل ۶ یک نمونه از ثبت دما و رطوبت در یک محیط آزمایشگاهی با استفاده از این دستگاه آورده شده است.



شکل ۵. دستگاه تله‌متری دما و رطوبت.



شکل ۶. نمونه داده‌های ارسال‌شده توسط دستگاه از محیط.

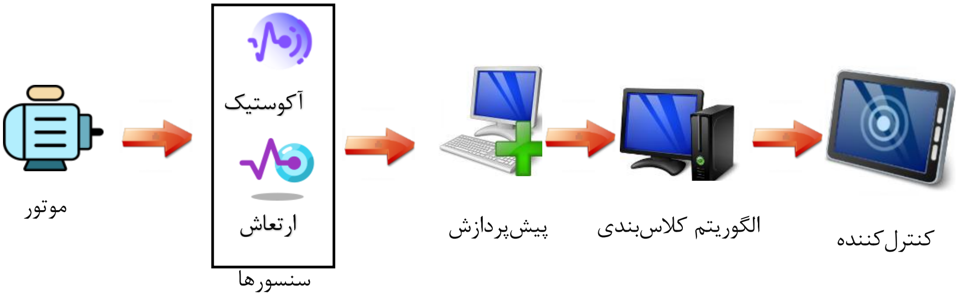
شکل ۷ یک دستگاه جمع‌آوری فرکانس بالا را نشان می‌دهد که به‌منظور ثبت داده از یک مبدل آنالوگ به دیجیتال ۲۰۰ کیلوهرتز استفاده کرده‌ایم. این برد با کابل USB و از طریق یک برنامه دسکتاپ به لپ تاپ متصل می‌شود و اطلاعات از این طریق به نرم‌افزار متلب منتقل می‌شود. کلیه فرمان‌ها ازجمله شروع ثبت، نرخ ثبت داده، شماره کانال‌های ثبت داده و پایان ثبت از طریق برنامه دسکتاپ بین برد و لپ‌تاپ منتقل می‌شود. داده‌های ذخیره‌شده، قابلیت مشاهده و پردازش در نرم‌افزار اکسل را دارند. برد طراحی‌شده قابلیت ثبت ۸ کانال به‌صورت هم‌زمان را دارد، این برد به‌منظور ثبت داده‌های فرکانس بالا شامل ارتعاش و آکوستیک که به‌خصوص برای تشخیص عیب موتورهای کشاورزی مناسب هستند، استفاده می‌شود. در ساختار پیشنهادی کلیه فرایند ارسال داده، پایش وضعیت و پردازش داده به‌وسیله بردهای طراحی‌شده و الگوریتم‌های هوش مصنوعی انجام می‌شود که منجر به توسعه قابلیت‌های این پژوهش در کشاورزی هوشمند شده است.

شکل ۷. دستگاه ثبت داده‌های فرکانس بالا.

الگوریتم پردازش سیگنال و کنترل سرعت

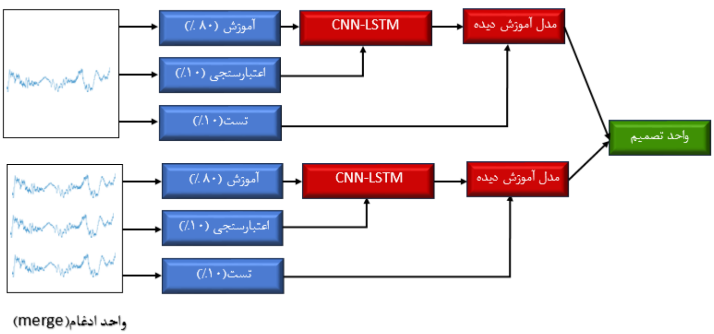
در این بخش، روش پیشنهادی تشخیص عیب و کنترل سرعت برای موتورها ارائه می‌شود. همان‌طور که در شکل ۸ نشان داده شده است، در ابتدا داده‌های ثبت‌شده پیش‌پردازش می‌شود، پیش‌پردازش داده شامل استفاده از فیلتر ناچ و تبدیل موجک است که به‌منظور حذف نویز و اغتشاش استفاده می‌شود. سپس داده‌ها وارد الگوریتم کلاس‌بندی می‌شوند و بر اساس داده‌های ثبت‌شده و الگوریتم‌های ارائه‌شده، شبکه آموزش داده می‌شود. پس از آن شبکه آموزش داده‌شده به‌منظور کلاس‌بندی داده‌های جدید استفاده می‌شود. در این حالت، در صورتی که موتور سالم باشد از کنترل‌کننده PID استفاده می‌شود و در صورتی که عیب تشخیص داده شود، از دو کنترل‌کننده PID استفاده می‌شود. مجموعه داده استفاده‌شده برای تشخیص عیب، پیچیدگی بسیاری دارد. در این حالت، فرکانس نمونه‌برداری برابر با ۴۲ کیلوهرتز و ثبت داده در بازه‌های ۱۰ ثانیه‌ای انجام می‌شود. به‌منظور ثبت داده‌های ارتعاش از سنسور PCB, model ۶۰۳C۰۱ استفاده می‌شود. سنسور ارتعاش اول به‌وسیله آهنربا به درایو موتور متصل می‌شود و سنسور ارتعاش دوم و سوم به محفظه بلبرینگ موتور متصل می‌شود. برای ثبت داده‌های آکوستیک از سنسور PCB, model ۱۳۰F۲۰ با فاصله ۲ سانتی‌متر از محفظه بلبرینگ قرار می‌گیرد. در این مجموعه داده از موتور ۳ اسب بخار استفاده شده و موتور در ۸ حالت مختلف شامل حالت سالم و ۷ عیب شامل عدم‌تعادل روتور، عدم تقارن روتور، سیم‌پیچی استاتور، عدم‌تعادل ولتاژ، خمیدگی روتور، میله‌های شکسته روتور و عیوب بلبرینگ درنظر گرفته شده است. همچنین این داده‌ها در ۳ سرعت مختلف و در

شرایط با بار و بدون بار ثبت شده است. داده‌های هر حالت معیوب در سرعت‌های مختلف و با بار و بدون بار در یک کلاس دسته‌بندی می‌شود. در این مقاله به‌منظور انتخاب بهینه شبکه عصبی عمیق از شاخصی که در الگوریتم ژنتیک به‌منظور انتخاب ساختار شبکه ارائه‌شده، استفاده می‌شود. پس از انتخاب ساختار بهینه شبکه، به‌منظور تعیین داده‌های بهینه تشخیص عیب از دو شاخص استفاده می‌شود که شامل دقت داده‌های آزمایش و زمان اجرای الگوریتم آموزش داده‌شده برای یک بسته ۱۰۰۰ تایی داده است. در این مقاله، اولویت انتخاب داده‌های ارتعاش یا آکوستیک برای تشخیص عیب، دقت و در صورت وجود مقدار دقت برابر یا نزدیک، داده‌هایی انتخاب می‌شوند که زمان اجرای شبکه به ازای آن‌ها کمتر باشد.



شکل ۸. الگوریتم تشخیص عیب و کنترل سرعت.

شکل ۹ فرایند آموزش شبکه عصبی عمیق را نشان می‌دهد. در ابتدا، داده‌ها به سه بخش تقسیم می‌شوند: ۸۰ درصد برای آموزش، ۱۰ درصد برای اعتبارسنجی و ۱۰ درصد برای آزمایش. ورودی شبکه به دو صورت است: در حالت اول هرکدام از سنسورها به صورت مجزا به شبکه داده می‌شود و در حالت دوم، داده‌های سنسورها ادغام می‌شود و به صورت سری به شبکه داده می‌شود.



شکل ۹. فرایند آموزش شبکه CNN-LSTM.

در این شبکه، به‌منظور کاهش حجم شبکه و تعداد پارامترها و با توجه به اینکه داده‌های ارتعاش و آکوستیک در یک بعد ارائه شده‌اند، از لایه‌های عصبی کانولوشنی (CNN) یک بعدی استفاده می‌شود. لایه‌های CNN برای استخراج ویژگی‌های مکانی از سیگنال‌های یک بعدی مناسب است. به این دلیل لایه‌های Maxpooling انتخاب شد که باعث کاهش ابعاد ویژگی‌ها می‌شود و از اضافه‌بار شبکه جلوگیری می‌کند، این لایه به‌جای Average pooling استفاده شد که ویژگی‌های برجسته سیگنال حفظ شود. لایه‌های LSTM به‌منظور استخراج ویژگی‌ها از داده‌های سری زمانی و به

منظور تعیین وابستگی‌های زمانی بعد از استخراج ویژگی مکانی استفاده می‌شود. به‌منظور طراحی بهینه شبکه، در لایه‌های آخر به‌منظور تعیین شماره کلاس از لایه‌های تمام متصل استفاده شده است. لایه Softmax برای تعیین توزیع احتمالات کلاس‌ها ارائه شده است.

به‌منظور دستیابی به ساختار بهینه برای شبکه عصبی عمیق که هم دارای کمترین تعداد پارامتر و زمان آموزش و همچنین دقت مناسبی باشد از الگوریتم ژنتیک استفاده می‌شود، الگوریتم استفاده‌شده به‌منظور بهینه‌سازی ساختار شبکه عصبی عمیق به‌صورت زیر نشان داده شده است:

۱- **تعریف فضای جستجو (کروموزوم‌ها):**

کروموزوم‌ها شامل پارامترهای شبکه شامل تعداد لایه، فیلترها و نرخ یادگیری هستند:

$$Chromosome = \{L_{CNN}\ , Layer\ \#\ i\ CNN(\ N_{kernel}, N_{unit}, p_i), L_{LSTM}, Layer\ j\ LSTM\ \left(\ N_{unit}, p_j\right), \eta\ \}$$

در رابطه بالا، L بیانگر تعداد لایه CNN و LSTM هست، N_{kernel}, N_{unit} بیانگر پارامترهای شبکه CNN و N_{unit} بیانگر پارامترهای LSTM است. همچنین p_i و p_j بیانگر مکان قرارگیری لایه‌های CNN و LSTM هستند، این دو عدد هیچ‌گاه برابر نخواهند بود، همچنین لایه LSTM در صورتی می‌تواند بعد از لایه CNN قرار بگیرد که قبل آن لایه MaxPooling 1D قرار گیرد. η بیانگر نرخ یادگیری الگوریتم است.

۲- **ایجاد جمعیت اولیه:**

یک جمعیت اولیه شامل مجموعه‌ای از کروموزوم‌ها به صورت تصادفی تولید می‌شود.

۳- **ارزیابی جمعیت:**

هر کروموزوم با مدل CNN-LSTM ایجادشده به‌وسیله تابع هزینه زیر ارزیابی می‌شود، در این تابع، اولویت اصلی دقت داده‌های آموزش و آزمایش است و پس از آن زمان آموزش و تعداد پارامترها در اولویت هستند:

$$\begin{aligned} Cost\ (k) = {} & (100 - \%Train\ accuracy) + (100 - \%Test\ accuracy) \\ & + 0.0005 \times Train\ time + 0.00003 \times \#\ parameters \end{aligned}$$

۴- **انتخاب**:

کروموزوم‌ها با استفاده از روش تورنمنت بر اساس مقدار $Fitness(k) = \frac{1}{Cost(k)}$ انتخاب می‌شوند.

۵- **جهش:**

در این حالت، پارامترهای تعداد لایه، اندازه فیلترها و شماره اولویت هر لایه باید عدد طبیعی ($\mathbb{N}$) باشند و مقدار نرخ یادگیری می‌تواند اعشاری یا عدد طبیعی باشد، همچنین پارامترهای شبکه هر لایه باید از اعداد توان ۲ انتخاب شود ولی اولویت و تعداد لایه می‌تواند از بین اعداد طبیعی انتخاب شود، در زیر از سه رابطه برای تعیین پارامترهای لایه‌ها استفاده می‌شود:

$$Mutation(N_{kernel}) = N_{kernel} + L, \qquad L \in \mathbb{Z}, \qquad N_{kernel} \in \mathbb{N}$$

$$Mutation(\eta) = \eta + \delta,\ \ \delta \in \mathbb{R},\ \ \eta > 0$$

$$Mutation(N_{unit}) = Choose\{2,4,8,16,32,64,\ldots\}$$

۶- تکرار:

این فرایند برای k نسل تکرار می‌شود تا بهترین معماری CNN-LSTM به‌دست آید.

مشخصات شبکه عصبی عمیق که با استفاده از الگوریتم بالا به‌دست می‌آید، به صورت جدول ۳ می‌باشد. پارامترهای نشان داده‌شده در جدول ۳ مربوط به حالتی است که از یک ورودی شامل داده‌های ارتعاش یا آکوستیک استفاده شود. در حالتی که از سه ورودی استفاده شده، واحد LSTM به‌منظور کاهش تعداد پارامتر به ۳۲ کاهش پیدا می‌کند.

جدول ۳. مشخصات شبکه عصبی عمیق استفاده‌شده.

Layer	Layer name	Kernel × unit	Specifications	#parameters	Layer	Layer name	Kernel × unit	Specifications	#parameters
۱	Conv 1D	5 × 64	Activation= ReLu, Strides=۱	۳۸۴	۸	MaxPooling 1D	-	Strides=۲	۰
۲	MaxPooling 1D	-	Strides=۲	۰	۹	LSTM	-	۶۴ Unit	۳۳۰۲۴
۳	Conv 1D	3 × 64	Activation= ReLu, Strides=۱	۱۲۳۵۲	۱۰	LSTM	-	۶۴ Unit	۳۳۰۲۴
۴	MaxPooling 1D	-	Strides=۲	۰	۱۱	Flatten	-	-	۰
۵	Conv 1D	3 × 64	Activation= ReLu, Strides=۱	۱۲۳۵۲	۱۲	Dense	1 × 32	Relu	۲۰۸۰
۶	MaxPooling 1D	-	Strides=۲	۰	۱۳	Dense	1 × 8	Softmax	۲۶۴
۷	Conv 1D	3 × 64	Activation= ReLu, Strides=۱	۱۲۳۵۲					

مدل ریاضی موتور و کنترل‌کننده PID

مدل موتور القایی به صورت (۳۲) و معادلات شار به صورت (۳۳) نشان داده شده است.

$$\begin{cases} V_{sd} = R_s I_{sd} + \dfrac{d\varphi_{sd}}{dt} \\ V_{sq} = R_s I_{sq} + \dfrac{d\varphi_{sq}}{dt} \\ V_{rd} = R_r I_{rd} + \dfrac{d\varphi_{rd}}{dt} - \omega_r \\ V_{rq} = R_r I_{rq} + \dfrac{d\varphi_{rq}}{dt} + \omega_r \varphi_{rq} \end{cases} \tag{۳۲}$$

$$\begin{cases} \varphi_{sd} = L_s I_{sd} + L_m I_{rd} \\ \varphi_{sq} = L_s I_{sq} + L_m I_{rq} \\ \varphi_{rd} = L_m I_{sd} + L_r I_{rd} \\ \varphi_{rq} = L_m I_{sq} + L_r I_{rq} \end{cases} \tag{۳۳}$$

که در آن V_{sd} و V_{sq} ولتاژهای اعمال‌شده به استاتور و I_{sd}، I_{sq}، I_{rd} و I_{rq} متناظر با محور d و q جریان استاتور و جریان روتور هستند. φ_{sd}، φ_{sq}، φ_{rd}، φ_{rq} شار استاتور و روتور هستند. R_s، R_r مقاومت‌های استاتور و روتور هستند. L_s، L_r به‌ترتیب نشان‌دهنده اندوکتانس استاتور و روتور هستند، در حالی که L_m اندوکتانس متقابل است.

معادلات بردار فضایی موتور القایی در قالب مرجع ثابت را نیز می‌توان بر حسب اجزای d-q به صورت ماتریسی (۳۴) نوشت.

$$\begin{bmatrix} V_{sq} \\ V_{sd} \\ V_{rq} \\ V_{rd} \end{bmatrix} = \begin{bmatrix} R_s + sL_s & 0 & sL_m & 0 \\ 0 & R_s + sL_s & 0 & sL_m \\ sL_m & \omega_r L_m & R_r + sL_r & \omega_r L_r \\ -\omega_r L_m & sL_m & -\omega_r L_r & R_r + sL_r \end{bmatrix} \times \begin{bmatrix} i_{sq} \\ i_{sd} \\ i_{rq} \\ i_{rd} \end{bmatrix} \tag{۳۴}$$

با انتخاب جریان‌های روتور و استاتور به‌عنوان متغیرهای حالت، (۳۵) به‌دست می‌آید.

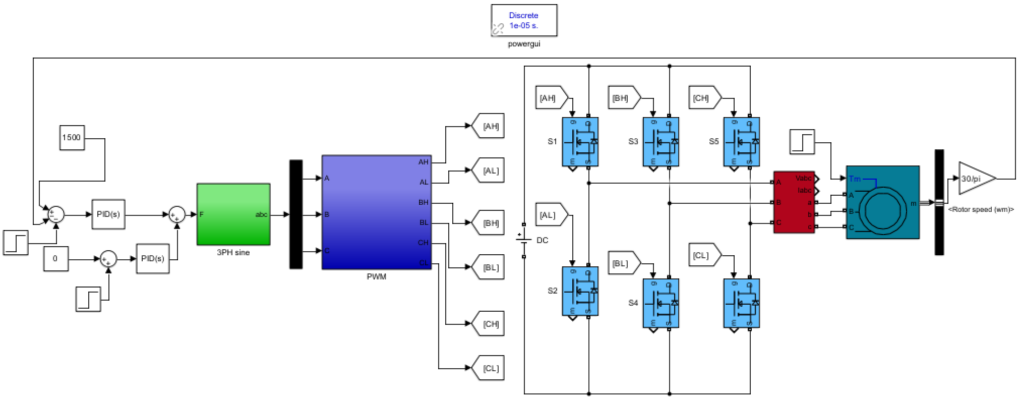
$$\begin{bmatrix} \frac{di_{sd}}{dt} \\ \frac{d_{isq}}{dt} \\ \frac{di_{rd}}{dt} \\ \frac{di_{rq}}{dt} \end{bmatrix} = \frac{1}{L_m^2 - L_r L_s} \times \begin{bmatrix} R_s L_r & -\omega_r L_m^2 i_{sq} & -R_r L_m & -\omega_r L_m L_r \\ \omega_r L_m^2 & R_s L_r & \omega_r L_m L_r & -R_r L_m \\ -R_s L_m & \omega_r L_m L_s & R_r L_s & \omega_r L_r L_s \\ -\omega_r L_m L_s & -R_s L_m & -\omega_r L_r L_s & R_r L_s \end{bmatrix} \times \begin{bmatrix} i_{sq} \\ i_{sd} \\ i_{rq} \\ i_{rd} \end{bmatrix} \times \frac{1}{L_m^2 - L_r L_s} \times \begin{bmatrix} -L_r & 0 \\ 0 & L_r \\ L_m & 0 \\ 0 & L_m \end{bmatrix} \times \begin{bmatrix} v_{sd} \\ v_{sq} \\ v_{rd} \\ v_{rq} \end{bmatrix} \tag{۳۵}$$

معادله گشتاور به‌صورت مکانیکی از (۳۶) و به‌صورت الکتریکی از (۳۷) به‌دست می‌آید.

$$T_e = J\frac{d\omega_m}{dt} + B\omega_m + T_L = \frac{J}{P}\frac{d\omega_r}{dt} + \frac{B}{P}\omega_r + T_L \tag{۳۶}$$

$$T_e = \frac{3}{2}P(\varphi_{sd} i_{sq} - \varphi_{sq} i_{sd}) \tag{۳۷}$$

که در آن، J اینرسی، B اصطکاک ویسکوز، T_L گشتاور بار، ω_r سرعت زاویه‌ای الکتریکی روتور برحسب رادیان بر ثانیه و ω_m سرعت موتور برحسب رادیان بر ثانیه است. که در آن P تعداد جفت قطب‌ها است. در شکل ۱۰ کنترل‌کننده سرعت موتور که در سیمولینک شبیه‌سازی شده، نشان داده شده است.



شکل ۱۰. کنترل‌کننده سرعت موتور.

نتایج و بحث

نتایج در سه بخش ارائه می‌شود: در حالت اول امنیت و کارایی پروتکل پیشنهادی ارسال داده‌های سنسورهای کشاورزی بررسی می‌شود، در گام بعد نتایج پردازش سیگنال ارائه می‌شود و در نهایت نتایج کنترل‌کننده ارائه می‌شود.

تحلیل غیررسمی پروتکل پیشنهادی

در این بخش به تحلیل غیررسمی پروتکل پیشنهادی خواهیم پرداخت و با دلیل و برهان نشان خواهیم داد که طرح پیشنهادی چه نیازهای امنیتی را برآورده می‌کند و در برابر حملات شناخته‌شده نیز مقاوم است. مزیت این طرح نسبت به مقالات ارائه‌شده در بخش پیشینه پژوهش [۵؛ ۹-۲۰] این است که مطابق جدول ۱، طرح‌های قبلی کلیه الزامات امنیتی را درنظر نگرفته‌اند، این مقاله با دو اثبات غیررسمی و رسمی، الزامات امنیتی را بررسی می‌کند و نشان می‌دهد پروتکل طراحی‌شده امنیت مناسبی دارد. همچنین این پروتکل در دسته پروتکل‌های سبک‌وزن قرار می‌گیرد که زمان اجرای کمی دارد.

- **تأمین نیاز امنیتی محرمانگی کامل رو به جلو**

در این نیاز امنیتی، فرض بر این است که اگر مهاجم قادر باشد به پارامترهای طولانی‌مدت مانند کلید خصوصی یا کلید محرمانه طرفین دست پیدا کند، نباید قادر باشد به کلید جلسه دسترسی داشته باشد. در پروتکل پیشنهادی، به دلیل وجود پارامترهای تصادفی x_i و y_i که در هر جلسه به‌روز می‌شوند، در کلید جلسه $SK_i = h(y_i||x_i||Y_j)$ وجود دارند. در نتیجه حتی اگر کلید محرمانه یا پارامترهای طولانی‌مدت نیز لو روند باز هم مهاجم قادر نخواهد بود به کلید جلسه دست پیدا کند.

- **تأمین نیاز امنیتی احرازهویت دوطرفه**

در پروتکل پیشنهادی، هر زمانی که یکی از موجودیت‌ها برای موجودیت دیگر پیامی را ارسال می‌کند، دریافت‌کننده پیام در ابتدا هویت ارسال‌کننده پیام را از طریق چک‌کردن برابری پارامترهایی مانند $U_i^* =? U_i$ ،$G_i^* =? G_i$، $Auth_g =? Auth_j$ و $M_i =? M_g$ بررسی می‌کند و از هویت ارسال‌کننده پیام اطمینان حاصل می‌کند؛ به همین دلیل می‌توان ادعا کرد که پروتکل پیشنهادی در این مقاله نیاز امنیتی احرازهویت دوطرفه را تأمین می‌کند.

- **مقاومت در برابر حمله دزدیده‌شدن تأییدکننده‌ها**

در این حمله، فرض بر این است که مهاجم ممکن است به حافظه دستگاه‌هایی که در اختیار موجودیت‌ها قرار دارد، نفوذ کند و به پارامترهای حساس دست یابد. در پروتکل پیشنهادی حتی اگر مهاجم به تلفن همراه کاربر دست پیدا کند، پارامترهای B_i، C_i ، w_i و q_i را به‌دست خواهد آورد که باز هم با استفاده از این پارامترها نخواهد توانست به کلید جلسه دست پیدا کند و پروتکل پیشنهادی ما در برابر این حمله نیز امن خواهد بود.

- **مقاومت در برابر حمله داخلی**

در این حمله، فرض بر این است که ممکن است شخصی در سمت گره دروازه وجود داشته باشد که سعی بر این دارد به رمز عبور کاربران دست پیدا کند. این در حالی است که در پروتکل پیشنهادی در مرحله ثبت‌نام، رمز عبور را به‌صورت واضح برای گره دروازه ارسال نکرده‌ایم و آن را در قالب $HId_i = h(id_i||pw_{U_i}||q_i)$ برای گره دروازه ارسال کرده‌ایم. به همین دلیل در صورتی که مهاجمی داخلی وجود داشته باشد، باز هم قادر نخواهد بود به رمز عبور کاربران دست پیدا کند.

- **مقاومت در برابر حمله تکرار**

در این حمله، فرض بر این است که مهاجم قصد دارد پیامی را به صورت تکراری برای طرفین ارسال کند. این در حالی است که در پروتکل پیشنهادی از مهرهای زمانی استفاده کرده‌ایم و زمانی که هر پیام توسط یکی از موجودیت‌های دریافت می‌شود، ابتدا با بررسی مهرهای زمانی تازگی پیام را بررسی می‌کند و در صورتی که موجودیت مور نظر از تازه‌بودن پیام مطمئن شد به ادامه ارتباط ادامه می‌دهد در غیر این صورت ارتباط خاتمه می‌یابد.

- **مقاومت در برابر حمله جعل هویت**

یکی دیگر از حملات شناخته‌شده در حوزه پروتکل‌های امنیتی حمله جعل هویت می‌باشد. در این حمله، فرض بر این است که مهاجم قصد دارد خود را به‌جای یکی از موجودیت‌های قانونی جا بزند و با دیگر موجودیت‌ها ارتباط برقرار کند. این در حالی است که در پروتکل پیشنهادی به علت اینکه زمانی که هر پیام به دست موجودیت‌ها می‌رسد، ابتدا احرازهویت صحیحی صورت می‌گیرد و مهاجم قادر نخواهد بود این حمله را در پروتکل پیشنهادی به کار ببرد.

تحلیل امنیتی رسمی پروتکل پیشنهادی

اسکایتر یک ابزار شناخته‌شده و قدرتمند برای تجزیه‌وتحلیل و شناسایی حمله‌های احتمالی و آسیب‌پذیری‌های پروتکل‌های امنیتی است. ابزار اسکایتر الگوریتم رمزنگاری و پروتکل‌های امنیتی طراحی‌شده را به‌طور خودکار تحلیل می‌کنند و رفتار آن را در مقابل بیشتر حمله‌های ممکن مورد بررسی دقیق قرار می‌دهد. شکل ۱۱، خروجی بررسی پروتکل پیشنهادی توسط اسکایتر را نشان می‌دهد.

Claim				Status	Comments
agriculture	user	agriculture,user1	Alive	Ok	No attacks within bounds.
		agriculture,user2	Weakagree	Ok	No attacks within bounds.
		agriculture,user3	Niagree	Ok	No attacks within bounds.
		agriculture,user4	Nisynch	Ok	No attacks within bounds.
		agriculture,user5	Secret idi	Ok	No attacks within bounds.
		agriculture,user6	Secret pwi	Ok	No attacks within bounds.
		agriculture,user7	Secret H(XOR(H(HB(bioi),idi,pwi,ai),H(pwi,HB(bioi)...	Ok	No attacks within bounds.
	gateway	agriculture,gateway1	Alive	Ok	No attacks within bounds.
		agriculture,gateway2	Weakagree	Ok	No attacks within bounds.
		agriculture,gateway3	Niagree	Ok	No attacks within bounds.
		agriculture,gateway4	Nisynch	Ok	No attacks within bounds.
		agriculture,gateway5	Secret gi	Ok	No attacks within bounds.
		agriculture,gateway6	Secret s	Ok	No attacks within bounds.
	sensor	agriculture,sensor1	Alive	Ok	No attacks within bounds.
		agriculture,sensor2	Weakagree	Ok	No attacks within bounds.
		agriculture,sensor3	Niagree	Ok	No attacks within bounds.
		agriculture,sensor4	Nisynch	Ok	No attacks within bounds.
		agriculture,sensor5	Secret sxj	Ok	No attacks within bounds.

Done.

شکل ۱۱. خروجی ابزار اسکایتر برای طرح پیشنهادی.

ویژگی Niagree بیان‌کننده این موضوع است که طرفین ارتباط موافقت می‌کنند که پیام‌ها به‌طور امن و با ترتیبی درست بین آن‌ها رد و بدل شده است. همچنین ویژگی Nisynch تضمین‌کننده این موضوع است که مهاجمین قادر به دستکاری پیام‌های رد و بدل شده نخواهد بود. همچنین ویژگی Alive در صورتی که تأیید شود بیانگر این موضوع است که طرح پیشنهادی در برابر حمله تکرار مقاوم است. همچنین ویژگی Weakagree تضمین می‌کند که در پروتکل، امکان جعل هویت وجود نداشته باشد. ویژگی Secret نیز تضمین خواهد کرد محرمانگی پارامتر مربوطه در پروتکل حفظ خواهد شد. همان‌گونه که در شکل ۱۱ قابل مشاهده است، طرح پیشنهادی معرفی‌شده در این مقاله، قادر است تمامی ویژگی‌های فوق را تأمین کند.

تحلیل کارایی طرح پیشنهادی

همان‌طور که مشاهده شد در طرح پیشنهادی از هیچ نوع رمزنگاری متقارن یا نامتقارن و عملگرهای سنگین‌وزن مانند ضرب اسکالر یا توان‌رسانی استفاده نشده است و صرفاً از تابع درهم‌ساز (هش) و عملگر XOR استفاده شده است که سربار زیادی از نظر محاسبات و صرف زمان ندارد. از طرفی بر اساس گفته امین‌طوسی[1] و همکاران [۲۲] که زمان اجرای هر عملگر را محاسبه کرده‌اند، هر هش زمانی (T_h) حدود ۰/۰۰۰۴ میلی‌ثانیه هر ضرب اسکالر (T_s) ۷/۳۵۲۹ میلی‌ثانیه، هر رمزنگاری متقارن (T_{sym}) ۰/۱۳۰۳ میلی‌ثانیه و هر عملگر فازی (T_F) ۰/۰۰۵۶ میلی‌ثانیه زمان خواهد برد

[1] Amintoosi

و از آن‌جایی که طرح پیشنهادی صرفاً از هش استفاده کرده است زمان اجرایی بسیار مناسبی نسبت به سایر طرح‌ها خواهد داشت که از رمزنگاری و عملگرهای سنگین‌وزن دیگر مانند ضرب اسکالر استفاده کرده‌اند. نتایج مقایسه زمان اجرای پروتکل در جدول ۴ نشان داده شده است.

جدول ۴. نتایج زمان اجرای پروتکل‌ها.

مقاله	عملگر	زمان (میلی‌ثانیه)
سونی و همکاران [۱۵]	$T_F + 6T_{ECC} + 31T_h$	۰/۱۲۰۶
لی و همکاران [۲۳]	$6T_{ECC} + 19T_h$	۰/۱۱۰۲
نیکروان و همکاران [۲۴]	$6T_{ECC} + 11T_h + 6T_{sym}$	۰/۸۸۸۸
الگوریتم پیشنهادی	$19T_h$	۰/۰۰۶۴

الگوریتم پردازش سیگنال و تشخیص عیب

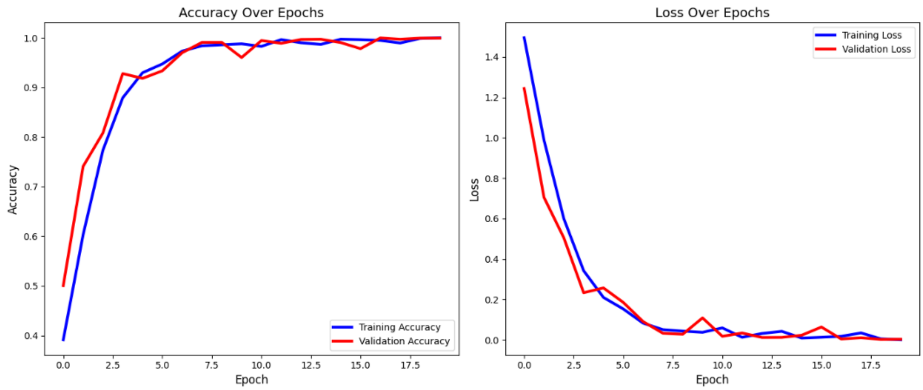
در این بخش، دقت الگوریتم تشخیص عیب و کنترل‌کننده سرعت موتور ارائه می‌شود. به‌منظور آموزش شبکه از ۲۱۵۰۳ داده، به‌منظور اعتبارسنجی ۲۶۸۸ و برای آزمایش از ۲۶۸۸ داده استفاده شده است. نتایج در جدول ۵ و شکل‌های ۱۵-۱۲ نشان داده شده است. در جدول ۵، A1 بیانگر سنسور ارتعاش اول، A2 سنسور ارتعاش دوم، A3 سنسور ارتعاش سوم و ACO سنسور آکوستیک است.

همان‌طور که در جدول ۵ دیده می‌شود، سنسور اول ارتعاش نتایج مناسبی برای تشخیص عیب داشته است. به علاوه، در حالتی که از ترکیب سنسورهای آکوستیک و ارتعاش استفاده می‌شود، دقت تشخیص عیب داده‌های آزمایش نسبت به حالتی که صرفاً از سنسورهای ارتعاش استفاده شود، بالاتر است. همان‌طور که در شکل ۱۲ و ۱۳دیده می‌شود، در حالتی که از ترکیب سنسورها استفاده شود، سرعت همگرایی و رسیدن به نتیجه دلخواه سریع‌تر است.

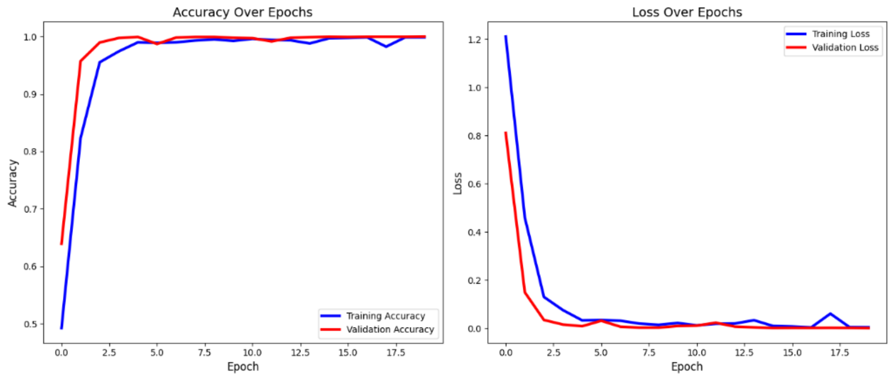
جدول ۵. نتایج کلاس‌بندی داده‌ها.

Sensors	Train accuracy	Validation accuracy	Test accuracy	Train time (sec)	Number of parameters
A1 [۴]	۸۵.۲۱	۸۴.۷۶	۸۴.۶۴	۳۰	-
A1 [۲۵]	۶۱.۴۴	۶۲.۲۰	۶۲.۶۱	۳۷۹	۴۲۵۰۴
A1	۱۰۰	۹۹.۹۳	۹۹.۹۲	۲۷۳۵	۱۰۵۸۳۲
A2	۹۸.۵۴	۹۷.۳۲	۹۷.۲۲	۲۷۱۶	۱۰۵۸۳۲
A3	۹۸.۶۰	۹۷.۱۴	۹۷.۷۶	۲۷۶۰	۱۰۵۸۳۲
ACO	۹۵.۸۵	۹۴.۹۰	۹۴.۹۷	۲۶۹۴	۱۰۵۸۳۲
A1, A2, A3 [۲۵]	۷۱.۷۸	۷۱.۹۸	۷۱.۱۳	۷۷۲	۱۰۵۹۹۲
A1, A2, A3	۹۹.۸۹	۹۹.۸۵	۹۹.۸۸	۵۹۶۸	۲۴۷۹۱۲
A1, A2, ACO	۹۹.۳۱	۹۹.۷۰	۹۹.۷۷	۶۳۳۵	۲۴۷۹۱۲
A1, A3, ACO	۹۹.۹۳	۱۰۰	۹۹.۹۶	۶۲۸۵	۲۴۷۹۱۲

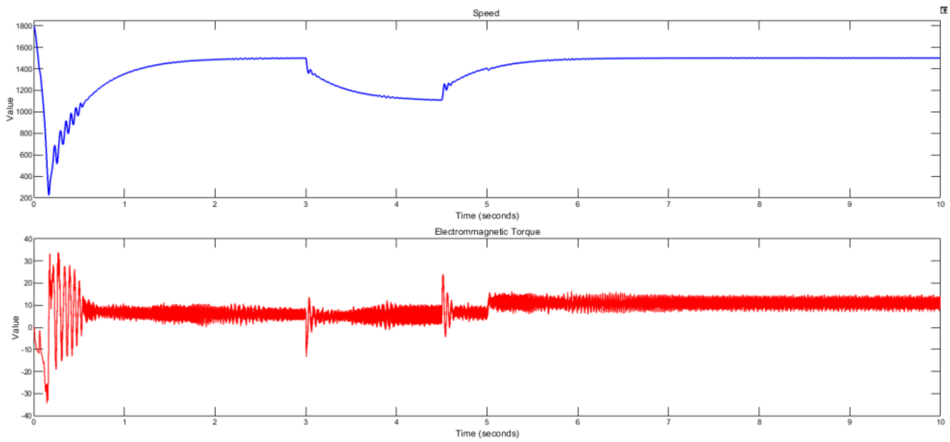
همان‌طور که در جدول ۵ دیده می‌شود، روش‌های قبلی، دقت مناسبی نداشتند و به‌صورت مؤثر برای تشخیص عیب در این مجموعه داده مناسب نیستند ولی با توجه به زمان آموزش کم، در مجموعه داده‌های ساده‌تر که به دقت مناسب برسند، کاربردی هستند.



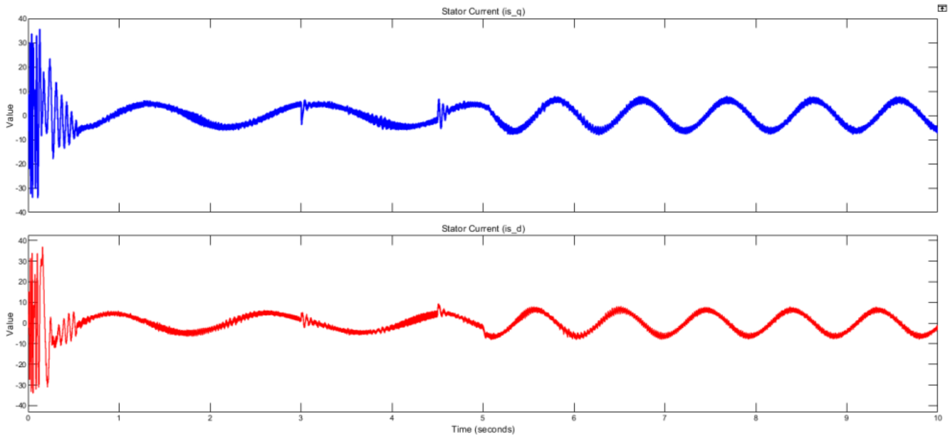
شکل ۱۲. نتایج کلاس‌بندی سنسور ارتعاش اول.



شکل ۱۳. نتایج کلاس‌بندی برای ترکیب سنسورهای ارتعاش اول و سوم و آکوستیک.



شکل ۱۴. سرعت و گشتاور موتور قبل و پس از وقوع عیب.



شکل ۱۵. جریان استاتور محور d-q قبل و پس از وقوع عیب.

در این مقاله برای کنترل سرعت موتور از یک کنترل‌کننده PID استفاده می‌شود، همان‌طور که در شکل ۱۴ مشاهده می‌شود، موتور از لحظه راه‌اندازی تا ۳ ثانیه سالم است، در این ثانیه عیب ایجاد می‌شود، سپس ۱.۵ ثانیه برای فرایند تشخیص عیب زمان لازم است و پس از تشخیص عیب، کنترل‌کننده تکمیلی وارد الگوریتم کنترلی می‌شود که منجر به کنترل سرعت پس از وقوع عیب می‌شود. در حالت ماندگار پس از عیب، کنترل‌کننده با افزایش گشتاور، سرعت موتور را در بازه دلخواه کنترل می‌کند. به علاوه، مطابق نتایج شکل ۱۵، پس از وقوع عیب و افت سرعت موتور به‌منظور کنترل سرعت موتور، نیاز به افزایش گشتاور است که منجر به افزایش جریان‌های موتور می‌شود. این افزایش جریان تا زمان جایگزین‌شدن موتور جدید یا اصلاح موتور معیوب وجود دارد. اصلاح عیب موتور در این مرحله، با توجه به اینکه در مراحل اولیه عیب هستیم، کم‌هزینه است و خطرات و آسیب‌های جانی کمتری دارد.

در این مقاله، یک ساختار جامع برای توسعه شبکه حسگری بی‌سیم در کشاورزی هوشمند ارائه شد. در کشاورزی هوشمند، یکی از عوامل مهم، هزینه است؛ طراحی سنسورها و کنترل کننده‌ها باید به‌گونه‌ای باشد که هزینه کمی داشته باشد و به تعداد زیاد توسط کشاورز قابل تهیه باشد، به‌منظور کاهش هزینه سنسورها از ریزپردازنده‌های ارزان استفاده می‌شود که قدرت پردازش بسیار زیادی ندارند. به علاوه، با توجه به گسترش کاربردهای اینترنت و ارسال داده‌ها به‌صورت بی‌سیم، نیاز به طراحی پروتکل‌هایی برای ارسال امن داده است. با درنظرگرفتن این دو عامل، این مقاله یک ساختار را ارائه داده است که از یک سخت‌افزار برای جمع‌آوری و ارسال داده‌های دما و رطوبت روی فضای ابری و همچنین یک پروتکل سبک‌وزن استفاده کرده است. مزیت اصلی پروتکل طراحی‌شده این است که علاوه بر درنظرگرفتن کلیه الزامات امنیت سایبری به‌منظور ارسال داده، زمان پردازش کمی دارد که باعث می‌شود مصرف انرژی کاهش پیدا کند و ارسال داده‌ها با نرخ سریع‌تری انجام شود. به‌منظور ارزیابی پروتکل طراحی‌شده، از نرم‌افزار اسکایتر استفاده شد، این نرم‌افزارها حالت‌های مختلفی که مهاجم می‌تواند به سیستم نفوذ کند را بررسی می‌کند و در صورتی که سیستم دارای نقص نباشد، در حوزه‌های مختلف پروتکل را تأیید می‌کند و این پروتکل در عمل قابل استفاده است.

بدین وسیله می‌توان اطلاعات محیطی را از نقاط مختلف ازجمله گلخانه و سایر زمین‌های کشاورزی دریافت و تحلیل کرد. در قسمت دیگر زیرساخت طراحی‌شده، به یکی از موضوعات و مشکلات پرتکرار صنعت کشاورزی پرداخته می‌شود. موتورهای استفاده‌شده در بخش کشاورزی پس از مدتی دچار عیب می‌شوند و با توجه به حفاظت ضعیف در مقابل اتصال به زمین برخی از زیربخش‌های کشاورزی، امکان وجود خطرات جانی و خطرات مالی ازجمله آتش‌سوزی هست. برخی

از مقالات به‌منظور تشخیص عیب از الگوریتم‌های یادگیری ماشین و الگوریتم‌های ترکیبی استفاده کرده‌اند [۴] که برای داده‌های با تعداد عیب کم مناسب است ولی برای مجموعه داده‌های پیچیده مناسب نیستند و دقت حدود ۸۵ درصد برای این مجموعه داده را دارند. در این حالت، تشخیص سریع عیب بسیار مهم است. به‌منظور جمع‌آوری داده‌های موتورهای کشاورزی از یک سخت‌افزار استفاده می‌شود و به‌منظور تشخیص عیب، از یک الگوریتم مبتنی بر شبکه عصبی عمیق استفاده شده که هرکدام از لایه‌های این شبکه به‌دقت و برای دستیابی به نتایج بهینه انتخاب شده است. به‌منظور دستیابی به ساختار بهینه شبکه عصبی عمیق که علاوه بر دستیابی به دقت آموزش و آزمایش موردنظر، دارای حداقل تعداد پارامتر باشد، از الگوریتم ژنتیک استفاده شده است و الگوریتم ژنتیک برای این کاربرد اختصاصی شده است. همچنین به‌منظور کنترل سرعت موتورها از یک الگوریتم مبتنی بر کنترل‌کننده‌های PID استفاده شده است که منجر به کنترل سرعت در موتور سالم و معیوب می‌شود.

نتیجه‌گیری

در این مقاله، هدف ما ارائه یک طرح پیشنهادی سخت‌افزاری- نرم‌افزاری امن برای شبکه‌های حسگر بی‌سیم مستقر در زمین‌های کشاورزی و محیط‌های گلخانه‌ای هوشمند بود که بتواند تمامی جنبه‌های امنیتی را درنظر بگیرد و از طرفی سربار زیادی به سیستم نیز وارد نکند. به همین دلیل یک پروتکل احرازهویت و توافق کلید برای شبکه‌های بی‌سیم مستقرشده در زمین‌های کشاورزی که از عملگرهای سبک‌وزن استفاده می‌کند ارائه دادیم و در ادامه اثبات کردیم که طرح پیشنهادی علاوه بر اینکه نیازهای امنیتی را تأمین می‌کند و در برابر حملات احتمالی مهاجمین نیز مقاوم است سربار زیادی را به شبکه وارد نمی‌کند و برای پیاده‌سازی عملی در محیط‌های کشاورزی که با محدودیت انرژی روبه‌رو هستند مناسب است. سپس دو سخت‌افزار برای جمع‌آوری داده‌های محیطی فرکانس پایین و فرکانس بالا با دو پروتکل مختلف ارسال داده پیشنهاد شد. پس از آن، به‌منظور هوشمندسازی فرایند پایش وضعیت، از یک شبکه عصبی عمیق برای کلاس‌بندی عیوب و کنترل سرعت موتور پمپ‌های کشاورزی و سیستم آبیاری استفاده شد. در این حالت نشان داده شد که روش ارائه‌شده و استفاده ترکیبی از سنسورهای ارتعاش و آکوستیک، نتایج مناسبی داشت. همچنین کنترل‌کننده توانست در حالت سالم و حالت با عیب، سرعت موتور را کنترل کند.

در پژوهش‌های آینده، از ترکیب شبکه عصبی عمیق کانولوشنی، یادگیری تقویتی و الگوریتم یادگیری فدراسیونی برای پردازش سیگنال استفاده می‌شود. همچنین به‌منظور بهبود کیفیت کنترل‌کننده و درنظرگرفتن قیود پژوهش در یک معادله از کنترل بهینه و تئوری مرتبه کسری استفاده می‌شود.

References

[1] Loghmanpour Zarini, R. (2022). Developing a Decision-Making Intelligent Software to Manage Mechanized Agricultural Operations and Measure its Performance in Paddy Tillage Operations. *Quarterly Scientific Journal of National University of Skills*, *18*(4), 49-71. https://doi.org/10.48301/kssa.2021.222590.1042

[2] Welbourne, E., Battle, L., Cole, G., Gould, K., Rector, K., Raymer, S., Balazinska, M., & Borriello, G. (2009). Building the Internet of Things Using RFID: The RFID Ecosystem Experience. *Institute of Electrical and Electronics Engineers Internet Computing*, *13*(3), 48-55. https://doi.org/10.1109/MIC.2009.52

[3] Dehghan, M., & Khosravian, E. (2023). Private Federated Learning for APT Detection in Internet of Drones. *Quarterly Scientific Journal of National University of Skills*, *20*(3), 465-484. https://doi.org/10.48301/kssa.2023.409787.2649

[4] Dehnavi, V. S., & Shafiee, M. (2023, December 26-28). *Inner and Outer Bearing Fault Diagnosis of electrical Motors Using a Proposed Algorithm and Vibration Signals*

[Conference session]. 14th International Conference on Information and Knowledge Technology, Isfahan, Iran. https://doi.org/10.1109/IKT62039.2023.10433018

[5] Itoo, S., Khan, A. A., Ahmad, M., & Idrisi, M. J. (2023). A Secure and Privacy-Preserving Lightweight Authentication and Key Exchange Algorithm for Smart Agriculture Monitoring System. *Institute of Electrical and Electronics Engineers Access*, *11*, 56875-56890. https://doi.org/10.1109/ACCESS.2023.3280542

[6] Pourbahrami, S., & Emadi, M. (2024). Cluster Head Selection Algorithm for Internet of Things in Wireless Networks based on the Density Peak Clustering. *Quarterly Scientific Journal of National University of Skills*, *21*(1), 91-107. https://doi.org/10.48301/kssa.2024.415637.2702

[7] Saini ,R. (2023, July 28-29). *A Lightweight Secure Authentication and Key Exchange Algorithm for Smart Agriculture Monitoring Systems* [Conference session]. 2023 International Conference on Data Science and Network Security, Tiptur, India. https://doi.org/10.1109/ICDSNS58469.2023.10245284

[8] Vangala, A., Roy, S., & Das, A. K. (2022, November 18-21). *Blockchain-Based Lightweight Authentication Protocol for IoT-Enabled Smart Agriculture* [Conference session]. International Conference on Cyber-Physical Social Intelligence, Nanjing, China. https://doi.org/10.1109/ICCSI55536.2022.9970603

[9] Das, M. L. (2009). Two-factor user authentication in wireless sensor networks. *Institute of Electrical and Electronics Engineers Transactions on Wireless Communications*, *8*(3), 1086-1090. https://doi.org/10.1109/TWC.2008.080128

[10] He, D., Gao, Y., Chan, S., Chen, C., & Bu, J. (2010). An enhanced two-factor user authentication scheme in wireless sensor networks. *Ad Hoc & Sensor Wireless Networks,*, *10*(4), 361-371. https://www.researchgate.net/publication/220419217_An_Enhanced_Two-factor_User_Authentication_Scheme_in_Wireless_Sensor_Networks

[11] Khan, M. K., & Alghathbar, K. (2010). Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks'. *Sensors*, *10*(3), 2450-2459. https://doi.org/10.3390/s100302450

[12] Vaidya, B., Makrakis, D., & Mouftah, H. T. (2010, October 11-13). *Improved two-factor user authentication in wireless sensor networks* [Conference session]. IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications, Niagara Falls, ON, Canada. https://doi.org/10.1109/WIMOB.2010.5645004

[13] Turkanović, M., Brumen, B., & Hölbl, M. (2014). A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion. *Ad Hoc Networks*, *20*, 96-112. https://doi.org/10.1016/j.adhoc.2014.03.009

[14] Chang, C. C., & Le, H. D. (2016). A Provably Secure, Efficient, and Flexible Authentication Scheme for Ad hoc Wireless Sensor Networks. *Institute of Electrical and Electronics Engineers Transactions on Wireless Communications*, *15*(1), 357-366. https://doi.org/10.1109/TWC.2015.2473165

[15] Soni, P., Pal, A. K., & Islam, S. K. H. (2019). An improved three-factor authentication scheme for patient monitoring using WSN in remote health-care system. *Computer Methods and Programs in Biomedicine*, *182*(1), 105054. https://doi.org/10.1016/j.cmpb.2019.105054

[16] Ali, R., Pal, A. K., Kumari, S., Karuppiah ,M., & Conti, M. (2018). A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture

monitoring. *Future Generation Computer Systems*, *84*, 200-215. https://doi.org/10.1016/j.future.2017.06.018

[17] Fatima, M. N., Obaidat, M. S., Mahmood, K., Shamshad, S., Saleem, M. A., & Ayub, M. F. (2023). Privacy-preserving three-factor authentication protocol for wireless sensor networks deployed in agricultural field. *ACM Transactions on Sensor Networks*, 1-20. https://doi.org/10.1145/3607142

[18] Alotaibi, M. (2018). An Enhanced Symmetric Cryptosystem and Biometric-Based Anonymous User Authentication and Session Key Establishment Scheme for WSN. *Institute of Electrical and Electronics Engineers Access*, *6*, 70072-70087. https://doi.org/10.1109/ACCESS.2018.2880225

[19] Moghadam, M. F., Nikooghadam, M., Jabban, M. A. B. A., Alishahi, M., Mortazavi, L., & Mohajerzadeh, A. (2020). An Efficient Authentication and Key Agreement Scheme Based on ECDH for Wireless Sensor Network. *Institute of Electrical and Electronics Engineers Access*, *8*, 73182-73192. https://doi.org/10.1109/ACCESS.2020.2987764

[20] Chen, M., Lee, T.-F., & Pan, J.-I. (2019). An enhanced lightweight dynamic pseudonym identity based authentication and key agreement scheme using wireless sensor networks for agriculture monitoring. *Sensors*, *19*(5), 1146. https://doi.org/10.3390/s19051146

[21] Khalid, H., Hashim, S. J., Ahmad, S. M. S., Hashim, F., & Chaudhary, M. A. (2021). Robust multi-gateway authentication scheme for agriculture wireless sensor network in society 5.0 smart communities. *Agriculture*, *11*(10), 1020. https://doi.org/10.3390/agriculture11101020

[22] Amintoosi, H., Nikooghadam, M., Shojafar, M., Kumari, S., & Alazab, M. (2022). Slight: A lightweight authentication scheme for smart healthcare services. *Computers and Electrical Engineering*, *99*(6), 107803. https://doi.org/10.1016/j.compeleceng.2022.107803

[23] Li, X., Niu, J., Bhuiyan, M. Z. A., Wu, F., Karuppiah, M., & Kumari, S. (2018). A Robust ECC-Based Provable Secure Authentication Protocol With Privacy Preserving for Industrial Internet of Things. *Institute of Electrical and Electronics Engineers Transactions on Industrial Informatics*, *14*(8), 3599-3609. https://doi.org/10.1109/TII.2017.2773666

[24] Nikravan, M., & Reza, A. (2020). A Multi-factor User Authentication and Key Agreement Protocol Based on Bilinear Pairing for the Internet of Things. *Wireless Personal Communications*, *111*(1), 463-494. https://doi.org/10.1007/s11277-019-06869-y

[25] Qian, L ,.Li, B., & Chen, L. (2022). CNN-based feature fusion motor fault diagnosis. *Electronics*, *11*(17), 2746. https://doi.org/10.3390/electronics11172746