Journal of Convergence for Information Technology
Vol. 11. No. 12, pp. 106-114, 2021

e-ISSN 2586-4440
DOI : https://doi.org/10.22156/CS4SMB.2021.11.12.106

A Study on the Use of Cognitive Radio Networks in the Military Operation Environment

Valentine Speybrouck[1], Eve Despoux[1], Yongchul Kim[2*]
[1]Student, Department of Electronic Engineering, Korea Military Academy
[2]Professor, Department of Electronic Engineering, Korea Military Academy

군 작전 환경에서의 인지 무선 네트워크 활용방안에 관한 연구

발렁틴 스페이브룩[1], 이브 데스포무랏[1], 김용철[2*]
[1]육군사관학교 전자공학과 학생, [2]육군사관학교 전자공학과 교수

Abstract The needs in terms of wireless communications are growing up both for civil and military applications. Therefore a constant improvement of this technology is required to meet customer wishes. One of its main shortcomings is the inefficient use of the spectrum in which a large part of the allocated bands of frequencies is unused. Since communication is crucial, spectrum shortage problems can lead a multi-national and coalition operation to failure. Cognitive Radio Networks (CRNs) are a promising technology which continuously analyses the spectrum searching for available frequencies. It can solve this spectrum issue by avoiding interferences, improving system-wide spectral efficiency, robustness to dynamic conditions and allowing more spectrum flexibility This paper specifically analyzed and presented the application of the CRNs in the military operational environment, and presented the appropriate method applicable to each actual operational situation.

Key Words : CRNs, Military Communication System, Frequency spectrum, Military operation, Spectral efficiency

요 약 무선 통신에 대한 요구는 민간 분야에서 뿐만 아니라 군 에서도 계속해서 증가하고 있다. 그러므로 무선 통신 기술의 개선이 사용자 요구에 부응할 필요가 있다. 무선 통신 기술의 활용에 있어서 주요 단점 중 하나는 할당된 주파수 대역의 많은 부분이 미 사용되는 스펙트럼의 비 효율적인 사용이라고 할 수 있다. 군 통신에 있어서 스펙트럼 부족 문제는 다국적 연합 작전과 같은 상황에서 성공적인 작전을 수행하는데 제한사항이 될 수도 있다. 이러한 문제점을 해결할 수 있는 방안으로 인지무선 네트워크는 실시간 사용 가능한 스펙트럼을 찾아서 사용할 수 있도록 해주는 중요한 기술이다. 또한 인지무선 네트워크 기술은 간섭을 피하고 시스템 전체의 스펙트럼 효율성을 개선하며 다양한 환경에서 유연성을 제공하는 등 스펙트럼 관련 문제들을 해결할 수 있다. 본 논문은 인지무선 네트워크의 군 작전환경에서의 활용 방안을 구체적으로 분석하여 제시하였으며 실제 작전 상황별로 적용 가능한 최적의 방안을 제시하였다.

주제어 : 인지무선 네트워크, 군 통신시스템, 주파수 스펙트럼, 군 작전환경, 스펙트럼 효용성

1. Introduction

The success of any military operation relies on the communication. Therefore the military needs a fast and safe communication system. The military is what we call a « primary user », it means that units have an allocated band they can use as they want and when they want. However

*This research was supported by Hwarang-dae research institute of Korea Military Academy in 2021
*Corresponding Author : Yongchul Kim(kyc6454@gmail.com)
Received October 24, 2021 Revised November 20, 2021
Accepted December 20, 2021 Published December 28, 2021

some situations require high data rates they cannot reach with their own bands and other frequencies such as UHF can be more appropriate for their applications [1]. This is one reason why the military develops and try to adapt CRNs to their use. But improving the spectrum utilization remains the main goal [2]. Obviously, messages and data transmission in the military Operation Environment are likely to be sensitive and the main issue of the use of CRNs in this context is the vulnerability. Interference, espionage, or various types of security vulnerabilities caused by spectrum sharing cannot be ignored and must be improved [3]. Likewise, the communication reliability, the high data rates, and the multi-hop cases are as well issues to take into account.

The present document consists in a comparison of CRNs' solutions in various military situations. It based on their abilities to respond to soldiers' needs and to support a range of services. It is organized as follow: first the main differences between military and civilian CRNs will be discussed. Then in a second part, an example of classification of the military CRNs will be exposed. Finally some scenarios where CRNs might be useful and a good alternative to other traditional means of communications will be provided and illustrate the classification.

2. Differences between military and civilian CRNs

2.1 Spatial and temporal variability

The first step to understand a future classification of CRNs for the military might be an analysis of the military needs and resources compared to the civil and commercial ones [4].

The network of antennas blend into the daily landscape such that we barely see them anymore. However, they reflect the massive infrastructure that civilians benefit for their wireless communication. Obviously, such facilities are not available in a military area of operation even if their wireless communication needs remain real. The military require communication between mobile platforms without any infrastructure. To compensate this lack of infrastructures, the military use multi-hop networks [5,6] as opposed to the one-hop civilian ones. A multi-hop network consists in multiple intermediate nodes that receive and transmit data via wireless links but not requiring common infrastructures or centralized control. Avoiding a single point of failure is indeed one of the main aim of the military CRNs. The benefits of multi-hop networks are many:

-The communication coverage area can be extended, thus solving the issue of temporal and spatial variability.

-A higher throughput leads to higher data rates which is a priority for military who need fast and efficient communications.

-Creating multiple short links requires less transmission power and energy and thus limiting interferences.

However, this multi-hop network scheme does not have a strong theoretical foundation yet. Currently, engineers struggle to extrapolate performances in one particular environment compared to networks requiring only single pairwise links.

To deal with the spatial and temporal variability the army does not settle for multi-hop networks, it goes beyond that with multiple heterogeneous networks in a same geographic area operating simultaneously. Yet, such networks are used in the commercial field but it does not deal with a dynamic environment which represents a significant difference with the military use. Multiple heterogeneous networks represents a real asset for the military. It would permit them to connect various unit echelon each other and the different networks could be adapted to solve security problems and increase the communication efficiency : if a network is under attack, another one can replace it so the mission will not be jeopardized. Similarly, if a piece of critical information has to be sent, the user can send it on every network so it will be sure that the recipient will have the information and the shortest deadlines.

It is worth noting that a multi-hop network with multiple variants simultaneously in a dynamic area is pointless for civilians and commercial. It means that any investment in research and development are done by marketing company, and the military have to do it themselves with fewer resources.

2.2. Security in an electromagnetic environment subject to jamming attacks

CRNs are still considered as an innovative way to communicate since they are still in the research step. In the meantime, the aggravating factors do not diminish since the proliferation of emitters keeps growing up while the spectral band assigned to the military is reducing. Added to jamming and electronic warfare attacks, the military cannot afford to misuse the spectrum [4]. Despite every solution discussed previously, military has to focus on what is essential like its safety for now, which means they must resort to only well-known communication techniques and not under development ones. To guarantee safe communications, the military must focus its efforts on short-term goals such as increasing the efficient use of the spectrum to have real-time information in a dynamic environment for instance. Or have a perfect knowledge of the spectrum availability at all times, be constantly aware of the spectrum use to detect jammers or any kind of threat and have more robust networks to keep communicating even under attacks.

A major part of the military's security threats listed above are not an issue for commercial and civilians [7]. This is why, despite some similarities in the use of CRNs, the Department of Defense is required to conduct most of its research without financial or technical support from the commercial sector.

To ensure the safety of military communications, it is important to keep in mind confidentiality, integrity, availability, and access control, which are the backbones of CRNs security common to all.

3. Classification of Military CRNs

The flexibility offered by the CRNs is undoubtedly one major asset for the military, they are eventually adaptable according to the environment, the battlefield and the mission. As previously detailed, the military requirements and the commercial ones are fairly different. This is why being able to implement their communication networks with such flexibility as spectrum sharing and spectrum accessing techniques for instance consist in a huge benefit.

To select one type of network as a military CRNs, the previous definition of the military operational requirements is crucial. As shown in Figure 1, the military CRNs can be divided into two cases where only the military frequency bands it owns or both military and civilian bandwidths are used.

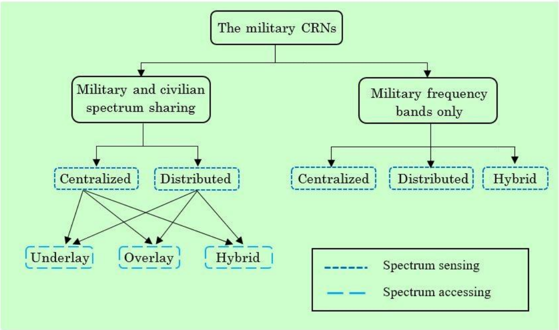


Fig. 1. Classification of Military CRNs

3.1 Military frequencies only

Let's assume that the military only communicates using frequencies already assigned to the military. In this case it's more difficult to distinguish primary users and secondary users because the military use CRNs to increase their spectrum bands not to establish a hierarchy between the users. Military frequencies only CRNs can be further divided into three cases. It is divided into centralized, distributed, and hybrid method.[1,8].

The first one is mainly based on a central node which communicates with every other nodes. It is responsible for the spectrum allocation for each user and the spectrum access authorization. Regarding the distributed network, also called decentralized network, it allows every user to communicate with each other horizontally, they are all free to exchange. While the centralized network enables a thin organization for the command chain, the distributed one allows a much better coordination between units. However, the centralized network is slightly more sensitive to jamming. Indeed, if a malicious user succeed in detecting the central node hence the whole network would be out of service because of this single point of failure. Similarly, distributed networks are more difficult to handle. For example, not all signals can be checked. It is also difficult to be sure that all SUs are communicating with trusted SUs.

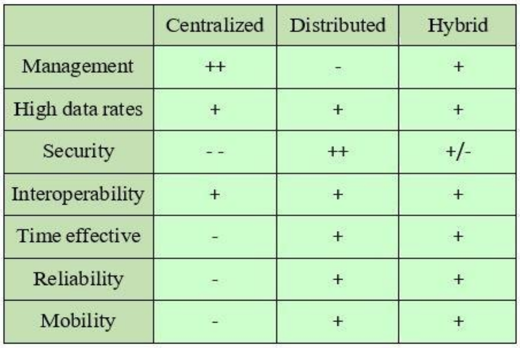
Both networks are quite time-consuming. One because the information must be assessed and must go through the central node, the other because of the information surplus, the time to make a decision might be longer. Centralized and distributed networks have both their pros and cons according to the military requirements even if the distributed one seems more appropriate and way more safe than the centralized one for the military.

Another alternative is to implement a hybrid network that combines both centralized and distributed systems. This kind of hybrid network gathers the best of both centralized and distributed networks and reduces the cons. The decentralized part might be suitable for tactical environment thanks to its mobility and the lack of infrastructure replaced by a multi-hop system extending the coverage radius. And the centralized part obviously eases the management of the whole network.

Regarding the spectrum accessing, there is no specification in the classification because the spectrum sharing occurs within the military bands. They are using the CRNs so everyone can access to a channel if there are too many soldiers for the military allocated bands. Thus, there is no priority issue and therefore no need to control the spectrum access.

All of these centralized, distributed and hybrid spectrum sensing specifications are listed and compared into the following table. The latter enhances all the hybrid scheme's qualities. The '+' sign represents good quality and the '-' sign represents bad quality. This table is specific to the military's networks needs which are significantly different from the civilian ones. This is why it should not be considered as a universal networks use.

Table 1. Overview table of networks' pros and cons



	Centralized	Distributed	Hybrid
Management	++	-	+
High data rates	+	+	+
Security	- -	++	+/-
Interoperability	+	+	+
Time effective	-	+	+
Reliability	-	+	+
Mobility	-	+	+

3.2 Military and civilian shared spectrum

Now, let's assume that the military needs to share frequency bands with civilians. Here the military are SUs among PUs, owners of licensed bandwidth. Once again the flexibility offered by CRNs allows the military to implement an overlay accessing technique or an underlay one [1].

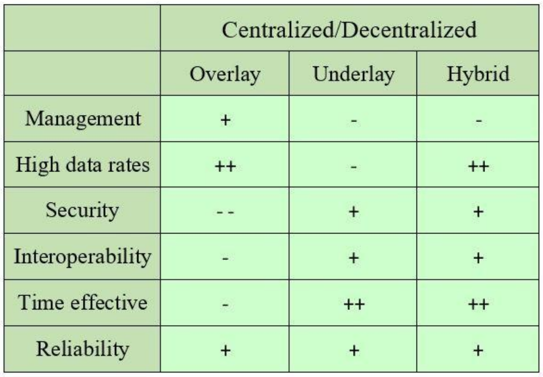
The overlay accessing technique prevents the SU from entering the network communication if it's already used by a PU. On the contrary, the underlay accessing technique allows both SU and PU to access the same band simultaneously but under power constraints to avoid interferences. The underlay accessing technique might be beneficial in term of security. Indeed, when the SU wants to communicate thanks to the underlay spectrum accessing, he will access the spectrum under the power constraints in order not to interfere with the PU. This power constraints consists in emitting only under the noise floor which means that the identity of the data sender will be hide, precisely because of this lack of power. This weakness for the underlay technique might finally become an asset so the military can use a civilian band by keeping their identity secret.

Again, one can easily imagined a kind of hybrid accessing technique using both overlay and underlay techniques [9]. Gathering benefits from both techniques, the hybrid scheme might be the best solution for the military in case of a shared utilization of civilians' bandwidth. Indeed, this particular scheme consists in using the overlay accessing technique but it might allow to switch from overlay to underlay in order to prevent the military to wait for a free spectrum in case of emergency.

Obviously, for each chosen dynamic accessing technique, the network can be centralized, distributed or hybrid with respect to the previous definitions. The most important thing is to think of a network that maximizes capacity. This is why the above overview table is provided, to summarize and compare the different types of accessing techniques.

Similarly to the previous table, the hybrid scheme is undoubtedly in general the most suitable option. Nevertheless, the study of the needs of the soldiers must be done in accordance with the mission they are currently performing.

Table 2. Overview table of accessing techniques' pros and cons



	Centralized/Decentralized		
	Overlay	Underlay	Hybrid
Management	+	-	-
High data rates	++	-	++
Security	- -	+	+
Interoperability	-	+	+
Time effective	-	++	++
Reliability	+	+	+

4. Practical scenarios

4.1 Military frequency only Scenario 1

Here is a situation requiring military frequencies only, within a hybrid network combining centralized and distributed networks. As previously seen, military multi-hop networks implemented thanks to CRNs seem to be necessary to military operations battlefield and meet soldiers' needs. They allow quick communications between elements without any infrastructures. Let's take the example of drones. Drones are either remotely controlled by soldiers or programmed to perform independent flights. It is aimed at collecting data or performing reconnaissance missions in hostile environments or on the battlefield. Thanks to CRNs and in particular multi-hop networks, a drone might be able to communicate with other drones and to work as a team to collectively carry out a mission.

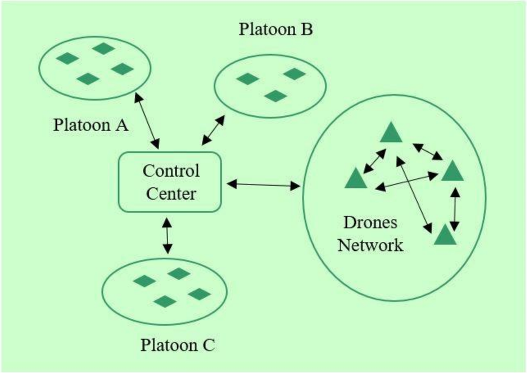


Fig. 2. Illustration of a hybrid network using military frequencies only

Let us imagine an operation in a foreign battlefield involving several drones that are working together among a reconnaissance company. If a drone is unfortunately destructed during the mission hence, thanks to the multi-hop technology, all intelligence and data gathered by the drone might be easily transferred to other drones. The mission can thus be continued.

Finally, the network can be fully distributed or distributed only for the drones and centralized for other elements as shown in Figure 2. However the multi-hop networks are quite safe, robust and they are rapidly implemented and easily managed. They can even be automatically carried out during a mission and deleted at the end.

4.2 Military frequency only Scenario 2

Fig. 3 shows the second scenario of military frequency only case. This scenario consists of military training involving a company of soldiers made up of two fighting platoons, a quick reaction force platoon and a resting platoon both at the base camp. An element of the air force is also involved in the training. The combined arms training takes place in the countryside with no civilians around. The military has its own allocated spectrum that must be shared with everyone, so some military personnel only have limited spectrum availability that does not allow for high data rates. Spectrum sharing can be a solution to counter this phenomenon. In fact, in this case, the military could utilize the spectrum of troops not currently deployed rather than the civilian band, which is the best solution to avoid interference and attacks from commercial users.

Therefore, the chosen solution for this situation would be to have the combat platoon use the resting platoon's band and the quick reaction platoon to use it over a distributed network using only military frequencies. In addition, to ensure the security of the communication in such an unsafe area with potential enemies or even jammers, the command decides to not use a Command Control Channel support but blind rendezvous schemes. Every soldiers involved in the communication network, at any level of the command chain, might be in receiver state but could change to be a sender, as soon as they have data to transfer. As a reminder, the decentralized aspect of the network might also ease the coordination between all users which are free to exchange information among themselves without going through the control center.

This scenario is especially thought to enhance the high level of security provided by CRNs and the ability of such networks to adapt to harsh conditions in unsafe areas. Also in this case, the spectrum sharing technology provided by the distributed network meets the military's high data rate requirements.

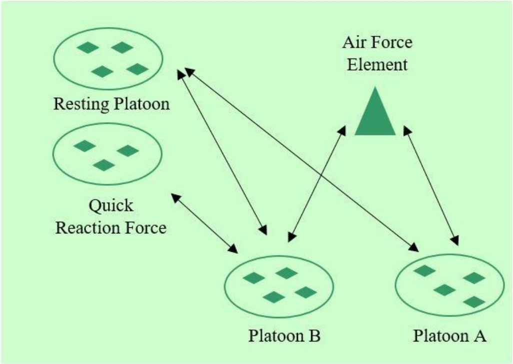


Fig. 3. Illustration of a distributed network using military frequencies only

4.3 Military and Civilian Shared Spectrum Scenario 1

This scenario is about a lost infantry team without any GPS or other way to locate themselves, they only have their regular radio. Unfortunately, they fail to communicate with anyone because they are too far away from their base as shown in Fig. 4. Thanks to CRNs and especially spectrum sharing, they might be able to establish a communication with anyone around them. The military generally avoid the interference with commercial bandwidth but during an emergency, if there is no free spectrum available in its own bandwidth, the military can choose to act as a SU in the commercial bandwidth.

To effectively tackle this situation, the military can choose to implement an hybrid network combining a main overlay spectrum access and a temporary underlay spectrum access. The underlay accessing technique enables the lost team to have a direct access to the civilian bandwidth. Power is certainly less important, but it has the advantage of being high enough to send an emergency message while still hiding a soldier's identity.

The use of the underlay technique can even become a security procedure for anyone who get lost. As soon as the commander and the soldier do not succeed to communicate with each other, after a predefined time-lapse, they should use the underlay scheme to establish a connection between them. Simply stated, they should use the dynamic hybrid sharing transmission mode of overlay and underlay which allow them to switch from overlay to underlay mode dynamically depending on the situation and the needs of the mission.

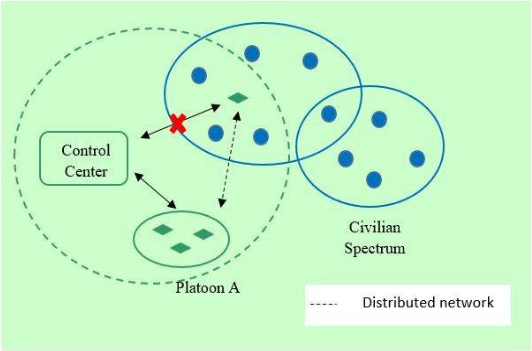


Fig. 4. Illustration of a spectrum sharing hybrid network

4.4 Military and Civilian Shared Spectrum Scenario 2

Figure 5 shows the second scenario of military and civilian shared spectrum case. This scenario is about a NATO military training involving several armies from different countries. This situation involves multiple heterogeneous networks in the same geographic area and so a robust scheme to counter the potential temporal and spatial variability due to this dynamic environment [10]. Regarding the massive population participating in this training, the use of CRNs seems necessary both to have access to a greater number of bandwidths but also to facilitate combined arms exchanges. In this situation, it would be desirable to use private bands available in the spectrum.

However, even if this is a training, the military must operate in safe conditions, especially for training of this scale. To ensure their communication safety, they use centralized network with an underlay spectrum accessing technique. As explained above, the underlay technique is very useful to improve the military stealth and not reveal their identity which is explicitly what they need here. They are not using a hybrid spectrum accessing which seems more effective as detailed in the previous scenario since it is way more complicated to implement because of its dynamic aspect so regarding the cost and means restrictions it is not useful for trainings.

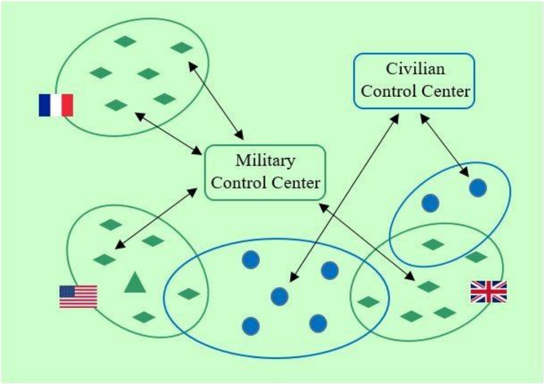


Fig. 5. Illustration of a spectrum sharing centralized network

5. Conclusion

As many other studies enhanced, CRNs are a high quality alternative to usual communication means. They are able to meet soldiers' needs notably in terms of security, interoperability, reliability or emergency in many cases. In addition, their high flexibility allows soldiers to adapt their communication network according to the situation, the lack of infrastructure, or the presence of a civilian spectrum. In this paper, we analyzed and presented the application of the CRNs in the military operational environment, and presented the appropriate method applicable to each actual operational situation.

REFERENCES

[1] B. Bharti, P. Thakur & G. Singh. (2021) A framework for spectrum sharing in cognitive radio networks for military applications. *IEEE Potentials*.

[2] T. J. Willink. (2007). SDR and Cognitive Radio for Military Applications. *Emerging Wireless Technologies*.

[3] A. G. Fragkiadakis, E. Z. Tragos & I. G. Askoxylakis. (2013). A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks. *IEEE Communications Surveys & Tutorials*.

[4] J. R. Agre, T. MacDonald, S. Shah & M. S. Vassiliou. (2013) Crucial Differences Between Commercial and Military Communications Technology Needs. *IEEE Military Communications Conference*.

[5] T. Braun, A. Kassler, M. Kihl, V. Rakocevic, V. Siris & G. Heijenk. (2009) Multihop Wireless Networks. *Traffic and QoS Management in Wireless Multimedia Networks*.

[6] T. Bräysy, B. Buchin, S. Couturier, J. Krygier, V. L. Nir, N. Smit, T. Tuukkanen & E. Verheul. (2018). Assessment of Cognitive Radio Networks through Military Capability Development Viewpoint. *International Conference on Military Communications and Information Systems* (ICMCIS).

[7] H. Tang & S. Watson. (2014). Cognitive radio networks for tactical wireless communications. *Defence R&D Canada, Scientific report*.

[8] H. Liu, Z. Lin, X. Chu & Y. Leung. (2012). Taxonomy and Challenges of Rendezvous Algorithms in Cognitive Radio Networks. *International Conference on Computing, Networking and Communications* (ICNC).

[9] Y. Chen, Q. Lei & X. Yuan. (2014). Resource allocation based on dynamic hybrid overlay/underlay for heterogeneous services of cognitive radio networks. *Wireless Personal Communications*.

[10] North Atlantic Treaty Organization. (2014) Cognitive Radio in NATO. *Science and Technology Organization*, January, 76-83.

스페이브룩 발렁틴(Valentine Speybrouck) [정회원]

· 2019년 9월 ~ 현재 : 프랑스 사관학교 전자공학 석사 과정중

· 관심분야 : 통신공학, 네트워크

· E-Mail : speybrouck.v@gmail.com

데스포무랏 이브(Eve Despoux) [정회원]

· 2019년 9월 ~ 현재 : 프랑스 사관학교 전자공학 석사 과정중

· 관심분야 : 통신공학, 네트워크

· E-Mail: speybrouck.v@gmail.com

김 용 철(Yongchul Kim) [정회원]

· 1998년 2월 : 육군사관학교 전자공학 (학사)

· 2001년 11월 : University of Surrey 전자공학(석사)

· 2012년 1월 : North Carolina State University 전자공학 (박사)

· 2012년 6월 ~ 현재 : 육군사관학교 전자공학 교수

· 관심분야 : 통신공학

· E-Mail : kyc6454@gmail.com