Information & Security

B. Bozveliev, S. Sotirov & T. Videv
vol. 43, no. 1 (2019): 35-44
https://doi.org/10.11610/isij.4303

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Generalized Net Model of Possible Drone's Communication Control Cyber Theft with Intuitionistic Fuzzy Estimations

Boris Bozveliev, Sotir Sotirov, Tihomir Videv

"Prof. Dr. Assen Zlatarov" University
"Prof. Yakimov" Blvd, Burgas–8010, Bulgaria
https://www.btu.bg/index.php/en/

ABSTRACT:

This article looks into the control of small, helicopter-like drones. They are more formally known as unmanned aerial vehicles (UAVs). Basically, a drone is a flying computerized machine that can be remotely controlled or fly autonomously through software-controlled flight plans in their embedded systems, working in conjunction with onboard sensors and a GPS receiver. Drones can be helpful or dangerous to us depending of their intended use. In the underlying study we use fuzzy estimations and, in this article, present a generalized net model of such a system and demonstrate the possibility of taking control over the communication between the transmitter and the receiver.

ARTICLE INFO:

RECEIVED: 10 JUN 2019
REVISED: 2 SEP 2019
ONLINE: 15 SEP 219

KEYWORDS:

generalized nets, UAV, radio transmitter, TX, radio receiver, RX, open TX, telemetry, fuzzy sets

Introduction

The current paper examines Generalized Net (GN) [1, 2] model of the possible cyber communication takeover of a remotely controlled drone UAV.[3] In order to control a UAV, we need some equipment, including a radio transmitter (TX) and a radio receiver (RX).

✉ Corresponding Authors: bozveli@gmail.com, ssotirov@btu.bg, tvidev@abv.bg

The Drone Radio Transmitter is an electronic device that uses radio signals to transmit commands wirelessly via a set radio frequency over to the Radio Receiver, which is connected to an aircraft that is being remotely controlled. In other words, this is the device that translates our commands into movement of the drone.

In some radios there is an option to connect an external transmitter module.

The Drone Radio Transmitter commonly use the following frequencies: 27MHz, 72MHz, 433MHz, 900MHz, 1.3GHz and 2.4 GHz 33 MHz, 900 MHz and 1.3GHz are typically used in long range FPV and RC systems.

27 MHz and 72 MHz ranges have been used in the past, but are rarely used nowadays. Equipment operating on those frequencies used crystals to bind the transmitter with a receiver.

2.4 GHz is the most popular frequency. Many controllers nowadays use Open TX firmware which is open source firmware for RC radio transmitters. The firmware is highly configurable and brings much more features than found in traditional radios. Open TX is a highly configurable system offering plenty options for all types of RC models. The main features of Open TX are: In flight audio/speech feedback, can store a large number of models on the radio, some logical switches and special functions can be programmed (low battery voltage, consumption, LUA scripts, direct flashing and more.

Telemetry is the data transmitted from the Radio Receiver back to the Radio Transmitter and it usually contains crucial information like, battery voltage reading, current draw and “RSSI” (Radio Signal Strength Indication).

This telemetry data can be displayed on the telemetry screen (in Open TX), and can also be customized as audio warnings.

The radio receiver is installed on the drone and it is capable of receiving signals from the radio transmitter, interpreting the signals via the flight controller where those commands are converted into specific actions controlling the aircraft. These receivers usually have the option of Telemetry (sending data back to transmitter) and Redundancy function (if two receivers are connected together and they lose connection and the second takes over).

To communicate, they use TX protocols between the radio transmitter and the radio receiver, and RX protocols between the radio receiver and flight controller.

TX Protocols are specific to some brands FrSky, Spektrum, Futaba, Hitec, Devo. And RX protocols are usually universal PCM, PWM, PPM, SBUS. They are also used by some specific brands like TBS, Graupner, FrSky, etc.

This basically means that a receiver must be compatible with a transmitter in order to establish communication. However, this may be not necessary. Frequencies should also be the same on both TX and RX receivers. For example, a 2.4 GHz receiver works only with a 2.4 GHz transmitter. In order to establish communication, the transmitter and receiver must be coupled. A drone radio transmitter transmits commands via channels. Each channel is an individual action command that is being sent to the aircraft. Throttle, Yaw, Pitch and Roll are the four main inputs required to control the drone. Each of them uses one channel, so there is minimum of four channels required.

Every switch, slider or knob on the transmitter uses one channel to send the information through to the receiver.

So at least six channels are used for the control of cheaper models and more on the high-end ones. In our model we are going to use common model 2.4 GHz controller with an Open TX firmware, with channels selection module and a protocol selection DB. We will show how the TX protocol is used to communicate with the receiver and also show how the signals are transmitted to the RX receiver, and a telemetry channel is established for RX for backwards communication with monitor exit on the transmitter controller that receives signals from the drone receiver. We are going to show how the UAV's processor is working and the signals flow in the system. It this model we are emulating an intruder who will possibly scan the 2.4 GHz communication and will try to take over any of the communication channels and protocols. Here our system is going to accumulate information from all input and output tokens and will send it to our intuitionistic fuzzy estimations algorithm and it will estimate whether the communication control is stolen from an intruder.

The possible communication intrusion may come from the interference of the communication between RX controller and TX receiver.[4]

The GN model allows us easily and clearly to understand the main mode of operation stages of the communication of the transmitter and the receiver of the drone and the possible intrusion, so then we may be able to improve security, troubleshoot and analyse better the whole process. In the above context we are going to evaluate the possibilities of the communication intrusion of the UAV's system. Here we are going to use fuzzy sets (IFS). The Intuitionistic Fuzzy Sets (IFSs)[5, 6, 7, 8] represent an extension of the concept of fuzzy sets, as defined by Zadeh,[9] with exhibiting function $\mu_A(x)$ defining the membership of an element *x* to the set *A*, evaluated in the $[0;1]$ interval. The difference between fuzzy sets and intuitionistic fuzzy sets (IFSs) is in the presence of a second function $\nu_A(x)$ defining the non-membership of the element x to the set A, where $\mu_A(x) \in [0;1]$ $\nu_A(x) \in [0;1]$, under the condition

$$\mu_A(x) + \nu_A(x) \in [0;1] \quad .$$

The IFS itself is formally denoted by:

$$A = \{\langle x, \mu_A(x), \nu_A(x)\rangle \mid x \in E\}.$$

We need (IFS), in order to evaluate the possible intrusion of the communication.

The estimations are presented by ordered pairs $< \mu, \nu >$ of real numbers from set $[0, 1]$, where:

$$\mu = \frac{S_1 + S_2}{S},$$

where:

S - All the possible TX- communication attempts.

S_1 - All the tokens from {L_3, L_6, L_9 } that enter in position L_{15}.

S_2 - The number of error attempts when the token in position L_{12} enters in position L_{16}.

$$\nu = \frac{S_3 + S_4}{S},$$

where:

S_3 - All the tokens from position{L_3, L_6, L_9 }that enter in position L_{16}.

S_4 - The number of error attempts when the token in position L_{12} enters in position L_{15}

S_5 - number of intruder attempts to take over communication.

S_6 - All the successful attempts made to take over communication.

S_7 - All the errors.

$$\pi = \frac{S_5 - S_6 - S_7}{S},$$

where:

The degree of uncertainty $\pi = 1 - \mu - \nu$ is all the packets of information in the communication that go to their destination and all the possible manipulated entries by an external source.

Communication Process Between a UAV Radio Transmitter TX and a RX Radio Receiver and Backwards Communication

Ultimately, TX transmitters facilitate communication between drone's RX receiver, and then the drone's processor processes the commands received by the transmitter, thus being able to complete the operations.

Initially the following tokens enter in the generalized net:

- in place L_1 - Λ - token with characteristic "User";
- in place L_2 - β - token with characteristic "Transmitter DB commands;
- in place L_8 - β'' - token with characteristic "Protocol processing database";
- in place L_{11} – β''' - token with characteristic "Channel processing database";
- in place L_{13} – χ - "Drone communication channel/protocol scanner";
- in place L_{14} – β'''' - token with characteristic "Receiver processing database";
- in place L_{19} – α - token with characteristic "Drone processor "
- in place L_{23} – δ- token with characteristic "IFS estimations $< \mu_k, \nu_k, \pi >$";

GN Model

GN model of common Communication process between a UAV radio transmitter Tx and a Rx radio receiver (Figure 1) is introduced by the set of transitions:

$$A = \{Z_1, Z_2, Z_3, Z_4, Z_5, Z_6, Z_7, Z_8\},$$

where the transitions describe the following processes:

- Z_1 = "Processing transmitter commands"

- Z_2 = "Processing communication protocols"
- Z_3 = "Processing channel selection"
- Z_4 = "External intrusion over the communication between transmitter and receiver"
- Z_5 = "Processing receiver commands"
- Z_6 = "Drone controller processing commands"
- Z_7 = "Flying drone"
- Z_8 = "Evaluation of the possible intrusion outcome over the communication of the UAV (drone)."

1. GN model of common Communication process between a UAV radio transmitter Tx and a Rx radio receiver and back-wards communication and possible external intrusion.

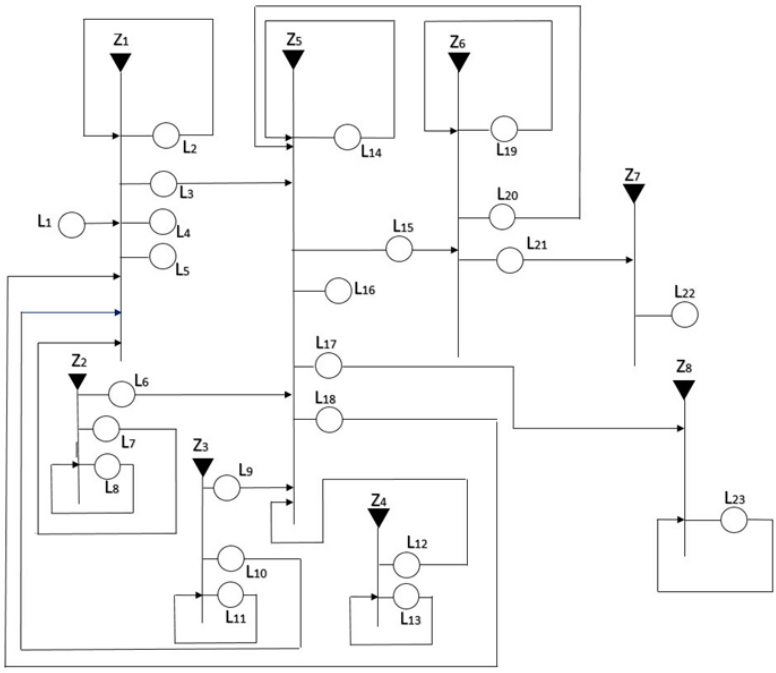

Figure 1. Generalized Net Model of Possible Drone's Communication Control Cyber Theft.

$$Z_1 = \langle \{L_1, L_2, L_7, L_{10}, L_{18}\} \{ L_2, L_3, L_4, L_5 \}, R_1, \vee (L_1, L_2, L_7, L_{10}, L_{18}) \rangle$$

$$R_1 = \begin{array}{c|cccc} & L_2 & L_3 & L_4 & L_5 \\ \hline L_1 & true & false & false & false \\ L_2 & true & true & W_{2,4} & false \\ L_7 & true & false & false & false \\ L_{10} & true & false & false & false \\ L_{18} & false & false & W_{18,4} & true \end{array}$$

where:

$W_{2,4}$ = "If there is an error with communications commands"

$W_{18,4}$ = "If there is a telemetry Rx signal error"

The token that enters place L_2 obtains the characteristic "Transmitter DB commands."

The token that enters place L_3 obtains "Communication command sent to receiver."

The token that enters place L_4 obtains the "Exit error."

The token that enters place L_5 obtains the characteristic "Transmitter audio/video screen."

$$Z_2 = \langle \{L_8\} \{ L_6, L_7 L_8 \}, R_2, \wedge (L_8) \rangle$$

$$R_2 = \begin{array}{c|ccc} & L_6 & L_7 & L_8 \\ \hline L_8 & true & true & true \end{array},$$

The token that enters place L_6 obtains the characteristic "Protocol command sent to transmitter."

The token that enters place L_7 obtains the characteristic "Protocol command sent to receiver."

The token that enters place L_8 obtains the characteristic "Protocol processing database."

$$Z_3 = \langle \{L_{11}\} \{L_9, L_{10}, L_{11}\}, R_3, \wedge (L_{11}) \rangle$$

$$R_3 = \begin{array}{c|ccc} & L_9 & L_{10} & L_{11} \\ \hline L_{11} & true & true & true \end{array},$$

The token that enters place L_9 obtains the characteristic "Channel selection command sent to receiver."

The token that enters place L_{10} obtains the characteristic "Channel selection command sent to transmitter."

The token that enters place L_{11} obtains the characteristic "Channel processing database."

$$Z_4 = \langle \{L_{13}\}\ \{L_{12}, L_{13}\},\ R_4,\ \vee (L_{13}) \rangle$$

$$R_4 = \begin{array}{c|cc} & L_{12} & L_{13} \\ \hline L_{13} & true & true \end{array},$$

The token that enters place L_{12} obtains the characteristic "External communication intruder."

The token that enters place L_{13} obtains the characteristic "Drone communication channel/protocol scanner."

$$Z_5 = \langle \{L_3, L_6, L_9, L_{12}, L_{14}, L_{20}\}\ \{L_{14}, L_{15}, L_{16}, L_{17}, L_{18}\},\ R_5,\ \wedge (L_3, L_6, L_9, L_{12}, L_{14}, L_{20},) \rangle$$

$$R_5 = \begin{array}{c|ccccc} & L_{14} & L_{15} & L_{16} & L_{17} & L_{18} \\ \hline L_3 & true & false & false & false & false \\ L_6 & true & false & false & false & false \\ L_9 & true & false & false & false & false \\ L_{12} & true & false & W_{12,16} & true & false \\ L_{14} & true & W_{14,15} & W_{14,16} & true & false \\ L_{20} & false & false & W_{20,16} & false & true \end{array},$$

where:

$W_{14,15}$ = "If there is a TX command sent OK"

$W_{12,16}$ = "If the intruder attack unsuccessful"

$W_{14,16}$ = " $W_{14,15}$ "

$W_{20,16}$ = "If there is a RX telemetry signal error"

The token that enters place L_{14} obtains the characteristic "Receiver processing database."

The token that enters place L_{15} obtains the characteristic "Successful translation of signal to processor."

The token that enters place L_{16} obtains the characteristic "Error/exit."

The token that enters place L_{17} obtains the characteristic "accumulated information form to-kens L_{15}, L_{16} - IFS estimate unknown."

The token that enters place L_{18} obtains the characteristic "Rx - backwards communication telemetry monitor."

$$Z_6 = \langle \{L_{15}, L_{19}\}\ \{L_{19}, L_{20}, L_{21}\},\ R_6,\ \wedge (L_{15}, L_{19}) \rangle$$

$$R_6 = \begin{array}{c|ccc} & L_{19} & L_{20} & L_{21} \\ \hline L_{15} & true & false & false \\ L_{19} & true & W_{19,20} & W_{19,21} \end{array},$$

where:

$W_{19,20}$ = "There is a telemetry RX back communication signal sent to the transmitter"

$W_{19,21}$ = "There is a translated command to the drone"

The token that enters place L_{19} obtains the characteristic "Drone processor."

The token that enters place L_{20} obtains the characteristic "Receiver telemetry."

The token that enters place L_{21} obtains the characteristic "Translated command into a drone manoeuvre."

$$Z_7 = \langle \{L_{21}\}\ \{L_{22}\},\ R_4,\ \vee\ (L_{21}) \rangle$$

$$R_7 = \begin{array}{c|c} & L_{22} \\ \hline L_{21} & true \end{array}$$

The token that enters place L_{22} obtains the characteristic "Drone is in operational state."

$$Z_8 = \langle \{L_{17},\ L_{23}\}\ \{L_{23}\},\ R_8,\ \vee\ (L_{17},\ L_{23}) \rangle$$

$$R_5 = \begin{array}{c|c} & L_{23} \\ \hline L_{17} & true \\ L_{23} & true \end{array},$$

where:

The token that enters place L_{17} obtains the characteristic "accumulated information form tokens L_{15}, L_{16} - IFS estimate unknown."

The token that enters place L_{23} obtains the characteristic "IFS estimations $< \mu_k, \nu_k >$."

Initially when no information has been derived from places L_4, L_{13}, L_{16} L_{17}, all estimates take initial values of $< 0, 0 >$.

When ≥ *0*, the current $(k+1) - st$ estimation is calculated on the basis of the previous estimations according to the recursive formula (as before):

$$< \mu_{k+1}, \nu_{k+1} >= \frac{\mu_k k + \mu}{k+1}, \frac{\nu_k k + \nu}{k+1},$$

where $< \mu_k, \nu_k >$ is the previous estimation, and $< \mu, \nu >$ is the latest estimation of the possible communication intrusion, for $\mu, \nu \in [0,1]$ and $\mu + \nu \leq 1$. In this way the token in place L_{21} forms the final estimation of the accumulated information from all the input and output tokens on the basis of previous and the latest events.

Conclusions

This is a common model of Open Tx firmware transmitter and its communication with a 2.4 GHz UAV receiver. The model is represented by a generalized net and shows the flow of the control in this wireless communication control system and the possible unwanted interference in control of the drone. So, the GN model helps us look further in the communication control of UAVs, and correct possible drawbacks with cyber security or simulate other problems or just use it for optimization of the behaviour of the wireless communication control over UAVs.

Acknowledgements

This work was supported by the Bulgarian Ministry of Education and Science under the National Research Programme "Information and Communication Technologies for a Digital Single Market in Science, Education and Security," approved by DCM # 577/ 17.08.2018.

References

[1] Krassimir Atanassov, *Generalized Nets* (Singapore, New Jersey, London: World Scientific, 1991).

[2] Krassimir Atanassov, Hristo Aladjov, *Generalized Nets in Artificial Intelligence: Generalized Nets and Machine Learning* (Sofia, Prof. Marin Drinov Publishing House,1998).

[3] Camille Alain Rabbath and Nicolas Léchevin, *Safety and Reliability in Cooperating Unmanned Aerial Systems* (World Scientific, 2010).

[4] Karl Iagnemma and Steven Dubowsky, *Mobile Robots in Rough Terrain: Estimation, Motion Planning, and Control with Application to Planetary Rovers* (Springer Science & Business Media, 2004).

[5] Krassimir Atanassov, "Intuitionistic Fuzzy Sets," Proceedings of VII ITKR's Session, Sofia, June 1983 (in Bulgarian).

[6] Krassimir Atanassov, "Intuitionistic Fuzzy Sets," *Fuzzy Sets and Systems* 20, no. 1 (1986): 87–96.

[7] Krassimir Atanassov, *Intuitionistic Fuzzy Sets: Theory and Applications* (Heidelberg, Germany: Physica-Verlag, 1999).

[8] Krassimir Atanassov, *On Intuitionistic Fuzzy Sets Theory* (Berlin: Springer, 2012).

[9] Lotfi A. Zadeh, "Fuzzy Sets," *Information and Control* 8 (1965): 333–353.

About the Authors

Boris Bozveliev has graduated from "Prof. Dr. Assen Zlatarov" University, Burgas, Bulgaria, Department of Computer Systems and Technologies. He has received his Master degree (2015.) and currently pursues a Ph.D. degree in the same university. His current research interests are in the field of security and communications.

Sotir Sotirov was graduated from the Technical University in Sofia, Bulgaria, Department of Electronics. He received his Ph.D. degree from "Prof. Dr. Assen Zlatarov" University, Burgas in 2005, and leads the University's "Intelligent Systems" Laboratory. His current research interests are in the field of neural networks.

Tihomir Videv has graduated from "Prof. Dr. Assen Zlatarov" University, Burgas, Bulgaria, Department of Computer Systems and Technologies. He has received his Masters degree in 2015 and is currently is working towards his Ph.D. degree in the same university. Tihomir's current research interests are in the field of smart-house, control and security.