INTUITIONISTIC FUZZY ESTIMATIONS OF IMPLEMENTATION OF PORT KNOCKING ON ROUTEROS

Ivelina Vardeva

ivardeva@gmail.com, ivardeva@btu.bg

ABSTRACT

The need for network security in today's increasingly digital and corporate world is now a must. In practice, all companies or organizations are forced to provide Internet services to their users. The present article describes a method for calculating intuitive fuzzy estimates to establish the network port security feature of port knocking, as a security builder for MikroTik communication devices via the RouterOS operating system. The practical application of generalized networks is a direction of research in the field of generalized networks, together with the theoretical studies of the connections between generalized networks and other concepts. Indexed matrices are used to describe the states of the token.

GNs MODEL

Network-based languages represent processes as networks. The process flow is easy to understand, but can be problems with abstraction. Most network languages are based on Petri nets and are used in process modeling. The theory of generalized networks was introduced by K. Atanassov as an extension of Petri nets. They are a tool for modeling flexible structures in which processes run in parallel over time. The generalized network is built of many transitions, containing conditions under which the nuclei pass from the input to its output places. As illustrated in Fig. 1, we will consider a GNs model containing four transitions, which correspond to the following aspects of the above described port knocking.

K represents the knockers' actions;

R represents the router actions;

L represents the lists of check actions;

E calculating of IFEs.

INTUITIONISTIC FUZZY ESTIMATIONS

Establishing secure implementation of port knocking connections is a process which depends on different factors, and is not always successful. This may depend on stability of the connection, closed connection by the client, the size and number of sent messages, syntax errors, denied request for policy reasons, etc.
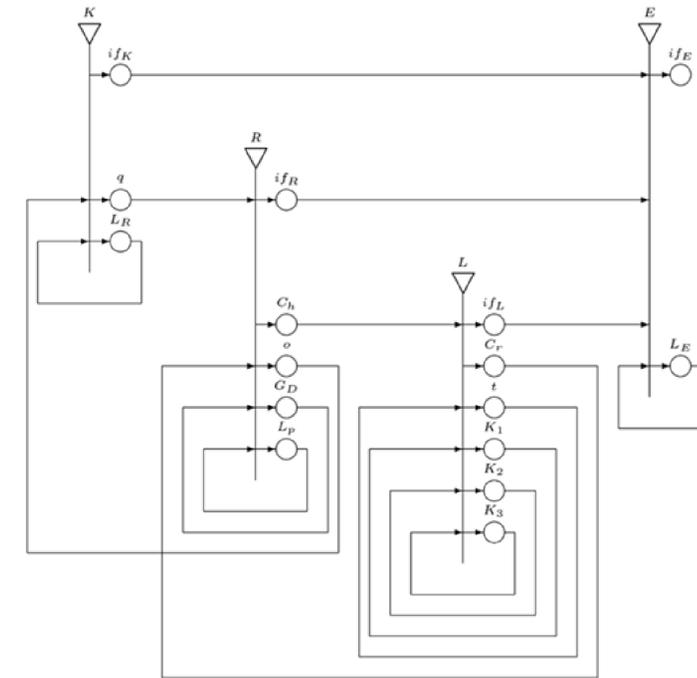

Fig. 1. Figure caption

For this reason, it is worth making certain estimations of past connection rates which can be taken into consideration in the current time moment.

Our estimations of establishing secure implementation of port knocking connections in each session are represented by ordered pairs $\langle \mu, \nu \rangle$ of numbers from the set [0; 1], where:

μ is the number of sent and confirmed packages divided by the total number of sent packages. The value of μ is calculated as $\mu = C/M$, where

M is number of all sent packages in the current session;

C is number of sent and confirmed packages in the current session.

ν is the number of sent and unconfirmed packages divided by the total number of sent packages. The value of ν is calculated as $\nu = C/M$, where

U is number of sent and unconfirmed packages in the current session;

The degree of uncertainty $\pi = 1 - (\mu + \nu)$ reflects the number of sent and received packages, which have not been yet confirmed by recipient, divided by the total number.

CONCLUSIONS

In this article was presented an intuitionistic fuzzy estimations as a part of generalized net model of implementation of port knocking. The presented GN model describes the port knocking represents a stealthy authentication system that employs closed ports to carry out identification of trusted users. The developed model can be used as a tool for research and analysis of processes occurring in communication devices. This novel method provides the means of establishing a connection to an application running on a completely isolated system on which no ports initially are open. In this article, we develop a GN model describing the performance of knocking on RouterOS ports. To provide remote access to non-public resources and services is limited to where resources can be accessed, use the port knock option and only access via virtual private network. The presented model can be used to study port knocking processes in the future.