Streszczenie

Wieloaspektowe modelowanie rozproszonych ataków odmowy usługi dla architektury Internetu Rzeczy

Niniejsza praca doktorska wpisuje się w gałąź informatyki związaną z badaniami nad bezpieczeństwem systemów w cyberprzestrzeni. Poruszana w niej problematyka badawcza dotyczy wieloaspektowej analizy rozproszonych ataków odmowy usługi (ang. Distributed Denial of Service (DDoS)) w środowisku Internetu Rzeczy (ang. Internet of Things (IoT)). Zaproponowana, wielopoziomowa analiza pozwala dobrać odpowiednie parametry sieci w celu minimalizacji skutków ataku przy jednoczesnej maksymalizacji żywotności sieci oraz zachowaniu odpowiedniego poziomu bezpieczeństwa. Na pracę doktorską składają się cztery artykuły naukowe.

Pierwszy z nich zawiera propozycję metodyki wykonywania pomiarów czynników związanych z bezpieczeństwem systemów informatycznych. Proponowane w artykule podejście rozszerza międzynarodowy standard ISO/IEC 27004 dotyczący pomiarów efektywności systemu bezpieczeństwa informacji o procedury walidacji i weryfikacji metod wykonywania pomiarów. Dzięki zastosowaniu nowego modelu możliwe jest uzyskanie powtarzalnych, miarodajnych pomiarów, które sprawiają, że określone na ich podstawie wskaźniki wydajnościowe służące do pomiaru efektywności mechanizmów bezpieczeństwa, są wiarygodne i niezawodne. Zastosowana metodologia oraz zebrane za jej pomocą miarodajne wskaźniki pozwalają na wykorzystanie ich w złożonym, heterogenicznym środowisku IoT, gdzie rzetelna ocena efektywności zastosowanych mechanizmów ochrony przeciwko atakom DDoS jest niezwykle istotna.

Drugi artykuł wprowadza ideę wieloaspektowej analizy bezpieczeństwa heterogenicznego środowiska IT. W ramach przedstawionej analizy zaproponowano nowe rodzaje analizy złożonych systemów, mianowicie analizę ekonomiczną oraz analizę emisji dwutlenku węgla. Wprowadzenie do wieloaspektowej analizy czynnika ekonomicznego umożliwia oszacowanie całkowitego kosztu utrzymania analizowanej architektury, podczas gdy za pomocą analizy emisji dwutlenku węgla można ocenić wpływ funkcjonowania danego systemu na środowisko naturalne. W artykule opisany został również przykład wieloaspektowej analizy centrum obliczeniowego. Zaproponowane, nowe analizy pozwalają na wybór mechanizmów, które są najbardziej wydajne pod względem ekonomicznym czy środowiskowym, co w nowoczesnych, rozległych i złożonych środowiskach IoT jest szczególnie istotne. Szerokie spojrzenie na badany system obecne w zaproponowanej analizie, w odniesieniu do ataków DDoS pozwala zwrócić uwagę na kilka ich aspektów jednocześnie. Takie podejście do problemu ataków DDoS pokazuje, że w środowiskach cechujących się dużą złożonością (jakimi są środowiska IoT) żaden z istotnych elementów nie może zostać pominięty.

Trzecia publikacja skupia się na analizie rozproszonego ataku odmowy usługi w warstwie percepcji Internetu Rzeczy, jaką jest bezprzewodowa sieć sensorowa (ang. Wireless Sensor Network (WSN)), wykonująca pomiary określonych charakterystyk zabytkowego budynku. W celu przeprowadzenia wieloaspektowej analizy ataku w artykule wykorzystano narzędzia wprowadzone w poprzednich pracach. Podczas analizy ataku DDoS dla przygotowanej sieci sensorowej został wykryty nowy typ ataku, który w publikacji określono mianem opóźnionego, rozproszonego ataku odmowy usługi (ang. Delayed Distributed Denial of Service (DDDoS)). Atak ten związany jest z wykorzystaniem zasobów energetycznych sensorów. Jak sama nazwa wskazuje, skutki tego ataku można zaobserwować dopiero po pewnym czasie, stąd może on powodować poważne konsekwencje, w szczególności w sieciach posiadających wrażliwe zasoby energetyczne.

Czwarta, ostatnia praca, koncentruje się na analizie warstwy percepcji IoT, jaką jest bezprzewodowa sieć sensorowa. WSN jako jeden z kluczowych elementów przemysłowych sieci Internetu Rzeczy, została w artykule wykorzystana do monitorowania inteligentnych sieci elektrycznych (ang. smart grid), również wchodzących w skład infrastruktury IoT. W artykule poruszony został problem bezpieczeństwa danych przesyłanych za pomocą sensorów, odpowiedniego ich rozmieszczenia na linii energetycznej, jak również doboru odpowiedniego algorytmu trasowania (ang. routing algo-

rithm). W pracy zaproponowano rozwiązanie pozwalające na zapewnienie poufności i dostępności przesyłanych danych przy jednoczesnej minimalizacji opóźnień czasowych występujących podczas transmisji.
Praca doktorska kończy się sformułowaniem konkluzji oraz określeniem dalszych kierunków rozwoju badań opisanych w powyższych publikacjach.

Abstract

Multilevel Modeling of Distributed Denial of Service Attacks in the Internet of Things Networks

Presented PhD thesis constitutes the branch of computer science research dedicated to cybersecurity. The discussed research objectives concentrate on multi-aspect analysis of distributed denial of service attacks (DDoS) in the Internet of Things environment and on providing the tools that will allow for choosing the most appropriate parameters of the network in order to reduce the impact of the attack on system performance, increasing the length of the proper network operation and ensuring the required level of security at the same time. The PhD thesis consists of four scientific papers.

The first one describes a new methodology of security measurements. The proposed approach extends the methodology of measuring the effectiveness of security systems available in ISO/IEC 27004 standard, by providing the procedures for validation and verification of measurement methods. By using the new model, it is possible to obtain repeatable and reliable measurements. The performance indicators (which are used to measure the effectiveness of security mechanisms) defined on the basis of the obtained measurements, are as well reliable and robust. The utilized methodology and obtained meaningful indicators can be thus applied in a complex, heterogeneous IoT environment, where the reliable assessment of the effectiveness of the protection mechanisms against the DDoS attacks is of vital importance.

The second article introduces the idea of multi-level analysis of the security of complex IT environments. The analysis proposes new methods of the examination of complex systems, namely the economic and the environmental analyzes. The introduction of the economic factor into the multi-aspect analysis allows to asses the total cost of maintenance of the considered IT architecture, while the analysis of the carbon dioxide emissions helps to determine the influence of the system performance on the natural environment. In the article, the case study of the multi-level analysis of the data center was discussed. The proposed methodology of multi-aspect analysis allows to choose the mechanisms, that are the most cost-effective in terms of finance or the influence on environment, which, in modern, widespread and complex IoT environments is particularly important. With regard to the DDoS attacks, a broad view of the considered system present in the proposed analysis, allows to draw attention to several of DDoS aspects simultaneously. Such an approach to DDoS attacks indicates that in highly complex environments (such as IoT environments) none of the essential elements can be omitted.

The third publication constituting the PhD thesis focuses on the analysis of distributed denial of service attacks in a perception layer of the IoT network, that is, the wireless sensor network, which measures some physical characteristics of the ancient building. In order to conduct the multi-aspect analysis of the attack, in the article the tools and methodologies proposed in previous research were utilized. During the analysis of the attack, a new type of DDoS, which in the publication is referred to as the delayed distributed denial of service (DDDoS) attack, has been discovered. The attack concerns the exhaustion of energy resources of sensor devices. As its name itself suggests, the effects of the attack can be observed only after some time, which can cause some serious consequences, especially in energy constrained networks.

The fourth, last paper, concentrates on the use of a perception layer of an IoT network, which is the wireless sensor network. The WSN, as one of the key elements of the industrial Internet of Things networks, in the article was used to monitor smart grid environment, being just another part of the IoT infrastructure. The publication deals with the problem of the security of the data being transmitted by sensors, their proper placement on a transmission power line, as well as on the choice of the right routing algorithm. A solution proposed in the article allows ensuring the confidentiality and availability of the transmitted data, minimizing time delays that occur during the data transmission at the same time.

The PhD thesis concludes with defining directions for potential development of the research descri-

bed in the above mentioned papers.