Information Protection Method in Distributed Computer Networks Based on Routing Algorithms

[1]Ahmad AbdulQadir AlRababah, [2]Bandar Ali Alghamdi

[1]Faculty of Computing and Information Technology in Rabigh, Rabigh 21911, KSA. King Abdulaziz University
[2]Faculty of Computer Study, Arab Open University, KSA Branch

Abstract
The Methods of protecting information during its transmission in distributed networks under the influence of deliberate attacks is very important and required. Based on the developed application "routable service", it allows solving the protection task without using encryption algorithms. Routing algorithms are used to determine the best path for packets from the source to the receiver and are the basis of any routing protocol. This paper describes concerning information transfer through public distributed networks under these deliberate attacks. The authors have developed «routed service» of data transmission through the distributed networks, allowing increasing information safety. The authors have simulated network attacks to the service and have calculated estimated probabilities of attacks. As results, «routed service» has been tested on the distributed network, network attacks on the service were modeled, and probabilities of attacks were estimated.

Key words:
distributed networks, network protocols, network attacks, routed based service, traffic multiplexing, Internet.

1. Introduction

In modern conditions, the main requirement of time for information technology is the affordable cost of implementation and ownership. Enterprises are looking for ways to reduce costs and improve the efficiency of their processes and systems, and this, in fact, promises technologies of distributed computing networks. This approach improves the efficiency of enterprise resources and offers a way to consolidate existing equipment in order to eliminate "white spots" of computers whose resources are not fully utilized yet [1]. You can create centralized pools of computing resources and distribute them in accordance with the priorities of the organization. The main idea of a distributed computing network is to provide computing as a utility. Users do not have to worry about where the actual data is or what computational processes they are accessing [3]. Users are interested in the ability to request information or calculations and get them in the right amount and at the right time. This is how the electrical network operates in the sense that people do not have to know where the generators are located and how the power lines are laid. Therefore, the goal can be formulated as follows: turn the calculations into a public service, accessible always and everywhere. Hence, the term "network of distributed computing"[2]. Of course, the approach to computing as a utility service corresponds to the view from the client. On the server side, that is, from the inside, the network of distributed computing is the allocation of resources, the distribution of information and the provision of a high degree of availability. Resource allocation means that everyone who needs resources or requests them will receive what they need. With the availability of free resources, requests cannot remain unsatisfied [4]. Distributing information means that the information needed by users and applications is delivered where and when it is needed. A high availability means that all data and calculations are available all the time just like Energy Company provides uninterrupted power supply [4, 5].

A distributed computing network is fundamentally changing the way enterprises use their resources, it virtualizes them. Resources become virtual, i.e. they can be distributed between the servers of the computing center, between the computing centers of the enterprise and between the enterprises themselves [7]. The main advantage is the provision of information at the right time, regardless of its location. To process information on any available resource, a distributed computing network must effectively distribute information between multiple systems, as well as provide access to data stored in heterogeneous systems, databases and file systems from different manufacturers [6, 8].

2. Research Methods and Related Works

In corporate networks, all elements belong to the same department, with the possible exception of communication channels. In such systems, it is possible to conduct a unified information security policy throughout the network. In public commercial networks, information distribution is at the forefront, and the protection of one's own information resources is mainly addressed at the user level [9]. Corporate networks can be connected to public networks. In this case, the administrations of corporate networks need to take additional precautions to block possible threats from public networks.

Manuscript received February 5, 2019
Manuscript revised February 20, 2019

Distortions of information represent a significantly greater danger. In many organizations, vital data is stored in files: inventory records, work schedules, order lists, bookkeeping, etc. If such data is distorted or erased, the work will be permanently paralyzed. The most dangerous thing is that in primitive cryptographic systems, the necessary distortions for this can be made without knowing the key. Therefore, serious ciphers must guarantee not only the stability of their non-disclosure, but also the impossibility of imperceptible modification of a single bit. Possession of the key opens up full access to the data, then you can compromise the research or design system, slightly distorting a dozen other numbers or removing information about the real state of affairs [10]. The most vulnerable to misrepresentation is economic information, where losses can be extremely large.

For the formulation of routing algorithms, the network is considered as a graph. In this case, routers are nodes, and physical lines between routers are edges of the corresponding graph. Each facet of the graph is assigned a specific number - the cost, depending on the physical length of the line, the speed of data transmission on the line or the cost of the line. In complex networks, there are always several alternative routes for transmitting packets between two stations. By route, we mean the sequence of routers that a packet must pass from the sender's station to the recipient's station [11, 13].

When executing a routing algorithm, a node should receive information from neighboring nodes that perform the same routing algorithm on networks that can be reached when data is transmitted through each neighboring node Fig.(1) [8]. By concentrating such information in the so-called routing tables, each node can determine the direction the data transfer route for each of the available networks. In the event that there are several such routes, the routing algorithm provides for the possibility of using a special criterion for choosing the optimal route for example, delaying the route by a separate packet, the number of intermediate routers passed. When a new packet arrives at the router, it extracts the network address, which is compared with the network addresses in the routing table [6, 14]. The line with the matched address indicates which nearest router should forward the packet to.

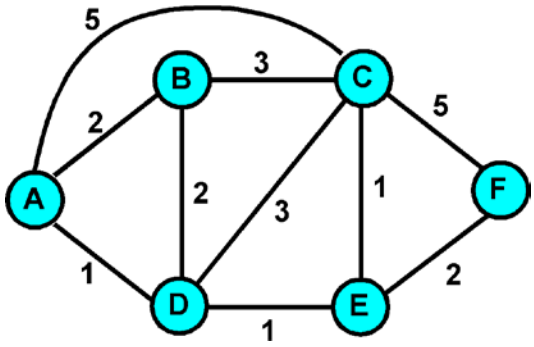


Fig. 1 Point-to-Point Routing Algorithms

With the increase in the number of routers, and, consequently, the number of subnets in large corporate networks, the number of entries in the routing table also increases. This leads to an increase in the time it takes to search for the necessary information in it, which in turn reduces the data transfer speed and leads to a decrease in the bandwidth of the network as a whole. A rational solution to this problem is the following table construction principle: only addresses of routers connecting this network with "neighboring" networks are entered into it, and all other networks are identified in the table by a special entry - the "default router" through which the path to all other networks passes [15].

3. Routing Alorithms: Fixed, Simple and Adaptive

If, when choosing a route, only the next (nearest) router was defined, then the routing is performed according to a distributed scheme - each router is responsible for choosing one route step, the entire route is the operation of all routers through which the packet passes. Such routing algorithms are called one-step.

Multi-step approach / source routing - The source node sets the complete route; there is no need to build and analyze tables. This speeds up the packet through the network, frees up the routers, but at the same time increases the load on the end nodes and used less often than in one step. However, in the new version of the IP protocol, along with the classic one-step routing, source routing will also be allowed.

One-step algorithms from the method of forming the routing tables are divided into classes: fixed (or static) routing algorithms; simple routing algorithms and adaptive (or dynamic) routing algorithms.

In fixed routing algorithms, all entries in the table are static. The network administrator decides on which routers to transfer packets with addresses, and manually (for example, using the route utility of UNIX or Windows NT) writes records to the table. The table is created during the

boot process; it is used before editing manually. Corrections are needed if the network fails the router and its functions are assigned to another. Distinguish between single-route tables, in which one destination is given for each destination, and multi-route tables, which define several alternative ones. In multipath tables, a route selection rule is specified, one path is the main path, and the rest are reserved. The algorithm is acceptable in small networks with a simple topology or to work on highways of large networks if the highway itself has a simple structure.

Simple routing algorithms do not use the routing table, or build it without the involvement of routing protocols. There are three types of simple routing:

- random, arriving packet is sent in a random direction, except the original one;
- avalanche routing, a packet is broadcast in all possible directions, except the initialone (similarly to the processing of frames with an unknown address by bridges);
- routing by previous experience, the choice is made according to the table, which is built on the principle of a bridge by analyzing the address fields of packets appearingon the input ports Fig.(2).

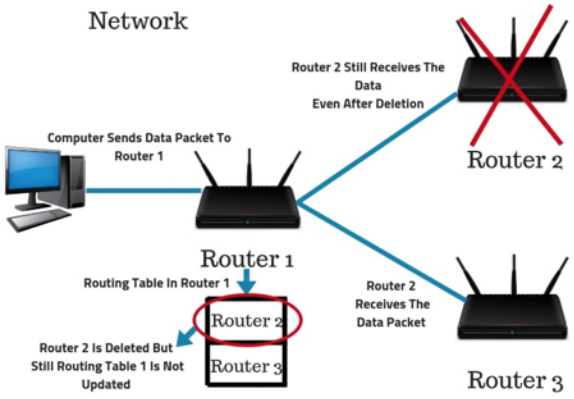


Fig. 2 Network Routing Algorithms schema

The most common adaptive (or dynamic) routing algorithm provides automatic updating of routing tables after network configuration changes. Protocols built on the basis of adaptive algorithms allow all routers to collect information about the topology of communications in the network, practicing all changes in the configuration of communications. The tables have information about the time interval during which the route will remain valid - the life of the route. Adaptive algorithms are distributed; all routers collect and summarize topological information.

There are three types of adaptive routing algorithms known as centralized, isolated and distributed. In the centralized algorithm, the central node gets all information about the networking topology, traffic and about other nodes. Only one node contains all the routing information Fig.(3). If the central node fails, the entire network fails. In isolation algorithm, the node gets routing information using local information. It does not require information from other nodes. In the distributed algorithm, the node receives information from the near nodes and finally decides the path to send the packet.

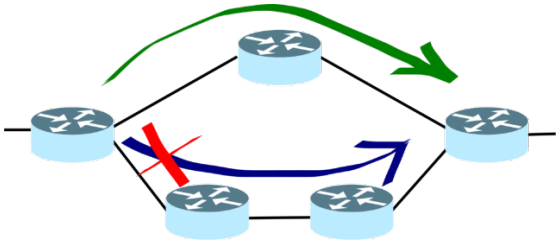


Fig. 3 Adaptive routing

Nowadays it is used route servers, by collecting routing information, and then distributing it upon requests to routers that are exempted from creating routing tables, or create only parts of these tables. There are special protocols for the interaction of routers with route servers, such as the Next Hop Resolution Protocol.

Adaptive algorithms must ensure the rationality of the route, be simple, so that their implementation does not waste too many network resources, in particular, they should not require too much computing or generate intensive service traffic, they must also have the property of convergence, that is, always lead to a unique result in an acceptable time. Adaptive routing information exchange protocols are divided into two groups, each of which is associated with one of the following types of algorithms:

- Distance Vector Algorithms, DVA
- link State Algorithms (LSA)

In distance-vector type algorithms, each router periodically and broadcasts a vector over the network, the components of which are the distances (the number of hops) from the given router to all the networks it knows about. Another metric is also possible, taking into account the number of intermediate routers and the time it takes for packets to go through the network between neighboring routers.

When receiving a vector from a neighbor, the router increases the distance to the networks indicated in the vector by the distance to this neighbor. After receiving a vector from a neighboring router, each router adds to it information about other networks it knows about, which it learned about directly (if they are connected to its ports) or from similar announcements from other routers, and then sends the new value of the vector again over the network.

In the end, each router learns information about all the networks on the intranet and the distance to them through neighboring routers.

In DVA, some disadvantages noticed regarding large networks, communication lines are clogged with intensive broadcast traffic, and configuration changes can be worked out according to this algorithm not always correctly, since they have only generalized information - the vector of distances, moreover, obtained through intermediaries. The operation of the router in accordance with the distance vector protocol resembles the operation of the bridge, since such a router does not have an accurate topological picture of the network.

The most common protocol based on distance vector algorithm is RIP, which is common in two versions - RIP IP, working with IP, and RIP IPX, working with IPX.

Link state algorithms provide each router with enough information to build an accurate network link graph. All routers operate on the basis of identical graphs, which make the routing process more resilient to configuration changes. Broadcast distribution (transmission of a packet to all immediate neighbors of the router) only may happen when the state of communications changes, which rarely happens Fig.(4). The vertices of the graph are the routers and the networks they join. Information distributed over a network consists of descriptions of various types of connections: router to router, router to network.

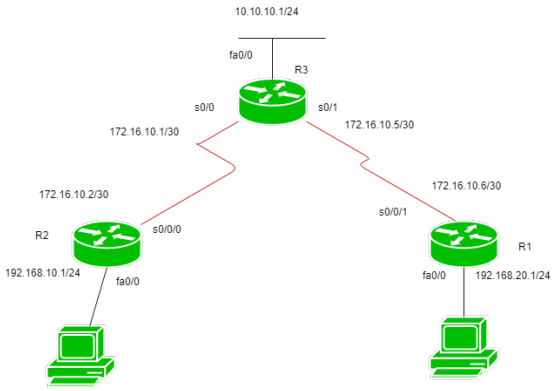


Fig. 4 Link state algorithm example

Protocols based on the link state algorithm are IS-IS (Intermediate System to Intermediate System) protocols of the OSI stack, OSPF (Open Shortest Path First) of the TCP / IP stack and the newly implemented Novell NLSP protocol.

4. The Proposed Method

This paper is developing the data sharing algorithms in distributed networks. The proposed method acts as an alternative to reducing computational costs when using encryption. The variety of threats affecting information in distributed networks is explained by the complex structure of the latter. Network attacks are many sided and are determined by a number of factors: the target of the attacker, the object of the impact, the architecture of the network segment. Currently, there are many works devoted to the classification and description of network attacks, including deal with threats that trap traffic in TCP / IP networks [16].

The most common classes of so-called active network attacks, for which the attacker needs to directly interact with some system that is part of the network [18]. The toolkit is just as wide: creating server overloads, exploiting protocol flaws, exploiting software vulnerabilities. In the international literature on information security, examples of such attacks can be found under the names “sniffing”, “flooding”, “spoofing”, “hijacking”, etc.

Existing measures to reduce the threat of attacks are effective, but, as a rule, highly specialized. For example, the use of cryptographic tools of the IP protocol makes the interception of TCP / IP packets impractical, but does not counteract attacks that cause significant traffic on certain sections of the traffic path [21].

The authors have developed a fundamentally different approach to increasing the stability of the system with targeted effects of an active nature. One type of active network attacks is the class of attacks based on sniffing. We give an example of one of them [19].

An attacker, having the knowledge that a certain organization regularly transmits data from A to G, can quite accurately determine the route from A to G at a time Δt and intercept on any of the traffic following the traffic (Fig. 5).

A, B, C, D, E, F, G - for the time being it should be understood as some nodal servers necessary for the spatial representation of the traffic route. So, A is the Internet gateway of the organization [20]. When sending tracing packets, the attacker at the time Δt determined the route of traffic (indicated by a dotted line) and launched an attack on the controlled router located on the BF leg [13,21].

The author has developed a “routable service” of SM data transmission through distributed networks. SM is a client-server application that allows the user to transfer data using a specific route. The nature of the route is determined by the base of SM criteria [22]. Among them, for example, delivery speeds, reliability, safety, etc.

This article describes the work devoted to the study of transmission safety criteria. Within the framework of the whole project, the rest were considered [23]. The role of routers for SM is a certain set of trusted servers of a distributed network. By a trusted server, we mean some multi-functional server of a distributed network to which an attacker does not have access.

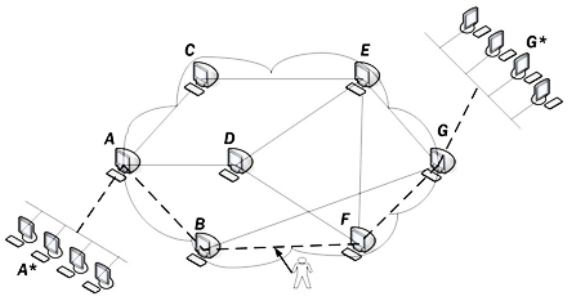


Fig. 5 Operation of routing protocols between A and G at the time of Δt

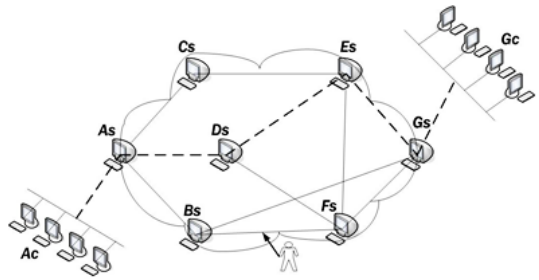


Fig. 6 Changing the route of traffic through the use of trusted servers DS, ES

On the trusted servers A_S, B_S, C_S, D_S, E_S, F_S, $G_S \in F$, the server part of the service is installed — SMS, which performs automatic "intelligent" traffic routing [24]. Denote by F - the set of all trusted servers with SMS, and F_j – specifically new trusted server i ∈[1,n].SMC is the application client-side service. SMC set poured into users' computers and provides users with a dialogue to initiate the data transfer process involving Fi (3).

In fig. 2 shows that the use of S_M made it possible to avoid traffic passing through the plot controlled by the attacker. This SM solution (final route) is probabilistic with the probability of taking p_j, $0 < p_j \leq 1, j \in [1, k]$, where k is the number of different routes from AS to GS on a graph with vertices A_S, B_S, C_S, D_S, E_S, F_S, GS and edges defined by the current network topology. The calculation of p_j values will be considered below.

There are various routes from AS to GS on the graph with vertices A_S, B_S, C_S, D_S, E_S, F_S and edges defined by the current network topology. The calculation of p_j values will be considered below [25].

Recall that in the process of transfer using SM, the data passes through a certain number of trusted servers, equal to f (for example in Fig. 6 f = 3). Each server is selected dynamically [26]. Given the above definition of routing tables for SMS, the choice of each next server describes the hypergeometric distribution of H_G $(c; a_i, n, c)$.

Distribution parameters: n - the number of all used trusted servers; c = 1, in the case of using the traffic multiplexing tool c> 1. a_i is the number of servers unavailable for F_i from among all servers (determined from the dynamic routing table M_i) [27]. But then it is logical to assume that inaccessible servers are not participating in the sample at each of the transfer stages. Thus, the final traffic route from the sender to the receiver when using S_M and f trusted servers (from n-available) will be chosen with probability:

$$p_j = \binom{n-a_0}{c} \times \binom{n-1-a_1}{c} \times \ldots \times \binom{n-f-a_f}{c}, \; j \in [1, k]; \tag{1}$$

a_i is the number of inaccessible servers for F_i at the moment of choosing F_i + 1 trusted server at i + 1 step.

$$a_i = n - \sum_{w=1}^{n} m_{iw}. \tag{2}$$

If multiplexing is not used, then

$$p_j = \binom{n-a_0}{c} \times \binom{n-1-a_1}{c} \times \ldots \times \binom{n-f-a_f}{c} = \frac{1}{n-a_0} \times \frac{1}{n-1-a_1} \times \ldots \times \frac{1}{n-f-a_f} \tag{3}$$

We divide all network attacks that the developed system can undergo into two classes: attacks on traffic between "adjacent" servers and attacks directly on trusted Fi servers. The notion of "adjacency" is determined dynamically for each transmission session, for example, "adjacent" are the F_t and F_t+1 servers selected on i and i+1 transfer stage $t \in [1, n]$, $i \in [1, f]$.

Let us estimate the likelihood of the first-class P_{A1} attack, when the attacker controls the area between the trusted servers F_t and F_t + 1. With an unknown spatial location Fi, we consider the attack successful if, during the operation of the C_M service, the transmitters F_t and F_t + 1 were selected at the i and i + 1 stage of transmission, $t \in [1, n]$, $i \in [1, f]$.

$$P_{A1} = \frac{2}{n-a_0} \times \frac{1}{n-1-a_1} + \frac{2}{n-1-a_1} \times \frac{1}{n-2-a_2} + \ldots + \frac{2}{n-(f-1)-a_{f-1}} \times \frac{1}{n-f-a_f} \tag{4}$$

Formula (4) easily extends to the case of plots controlled by an attacker between s-trusted servers F_t, F_t + 1, ..., F_t + s. Approximations (4) with the known relations of the parameters n, f, and a_i are considered in (3). Imagine a second, wider class of attacks in the form of an extraordinary (group) stream of events, i.e. sequences of events occurring one after the other at random intervals.

The fact that at the same time can come as several threats of different types or of the same type but from different sources, determines the originality of the flow.
Let ω denote the number of successfully attacked servers per unit of time (intensity).
Then the probability that attacks on m-trusted servers (of n available) will be realized during t is described by the Poisson distribution:

$$P_{A2}(m,t) = \frac{(\omega \cdot t)^m}{m!} e^{-(\omega \cdot t)} \quad (5)$$

To estimate ω, we use the results obtained in (4). The authors of this work used special COB-sensors (intrusion detection system) to register various types of network attacks on web servers. The results of the operation of COB-sensors are shown in Fig. 7
Imagine ω as the sum of the intensities of a finite number of different types of successful attacks, for example, such as spoofing, "man in the middle", flood, etc. . In this way,

$$\omega = \sum_{i=1}^{k} \omega_i = \sum_{i=1}^{k} p_i \cdot h_i \quad (6)$$

Pi is the probability of an attack of the i-th type, hi is the number of attacks of the i-th type,
$i \in [1, k]$. As the authors showed (4), it is almost impossible to give an exact estimate of ω, since its value depends on many factors: observation time, location of the server, functional purpose of the server, etc.

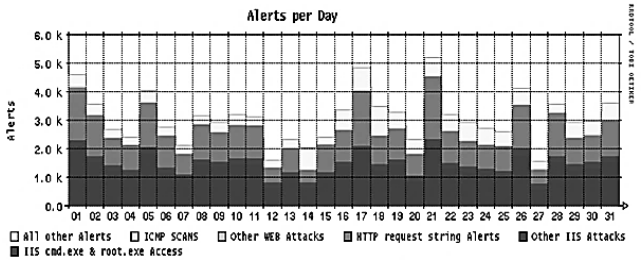


Fig. 7 The intensity of various types of attacks on monitored web servers

We will design a model of the flow of attacks that does not depend on the above factors (Fig. 8). In this scheme, the ordinary attack flow is modeled; the group flow model is constructed in a similar way.

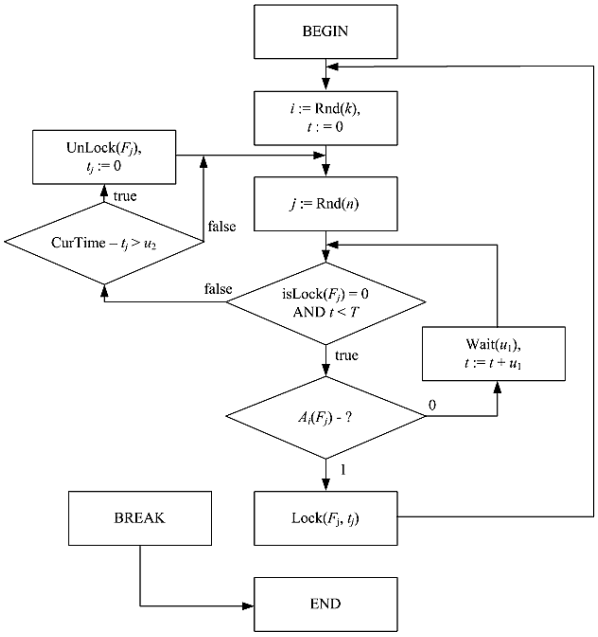


Fig. 8 Block diagram of the algorithm for generating the flow of attacks on trusted servers

We give the notation of variables and procedures used in the scheme.
Variables: n - the number of trusted servers in the network; k - the number of types of attacks; T is the duration of the selected type of attack; u_1 is the waiting time in case of an unsuccessful attack; u_2 - time to block trusted server in case of successful outcome of the attack; F - trusted server; p_i is the probability of an attack of the i-th species; i, j, t, t_j are auxiliary variables; CurTime is the current time.
Procedures and functions: Rnd (x) - generation of a random integer number on the interval [1; x], x> = 1; Unlock (F_j) - unlock the F_j server; A_i (F_j) - the outcome of the experiment "attack on the server F_j" determined by a discrete random variable with the distribution "the probability of taking the value of 1 (success) is p_i, the probability of taking the value of 0 (failure) is 1 - p_i"; Wait (x) - pause for time x; isLock (F_j) - returns the status of the F_j server (available; blocked); Lock (F_j, x) - lock F_j and return the current time to the variable x.
The work of the "routable service" application was tested on a global network of a large enterprise that fully simulates a distributed network. In (3), a description of the testing process is given, a graph of traffic routes is presented, and the probability of an attack occurring when using this application in a network is calculated. Based on the obtained results, it was concluded that the practical results corresponded to the theoretical concepts of the operation of the S_M service.
In formula (1), the possibility of embedding into S_M multiplexing algorithms is shown. Thus, it is possible to combine two approaches to ensuring the security of

transmitted information: on the one hand, to reduce the likelihood of an attacker accessing the communication channels used, and on the other, to apply a logical transformation of information. As a variant of the logical transformation, a system was developed in (1) that performs data separation across several separated transmission channels so that from a physical point of view, interception of all parts is difficult and the complexity of restoring the original sequence without any separate part of it is a maximum. In this paper, there are three main elements in the data separation system: a multiplexer, a demultiplexer, and transmitters. In function, the transmitters are close to trusted S_M servers. This fact creates good prerequisites for the integration of the two systems.

5. Conclusion

As a result of research, an algorithm for dynamic traffic routing has been developed. Based on this algorithm, a method was developed to protect the confidentiality of information in distributed networks - the “routable service” application. The main components necessary for the functioning of the system were developed. Estimates are given for the probabilities of the network attacks implementation on the transmitted information in the case of the use of a “routed service”. The service has been tested on the global enterprise network.
Using S_M's “routed service” to transfer data across distributed networks significantly reduces the likelihood of an attacker’s class of active network attacks without using any encryption tools.

Acknowledgment

We would like to thank Arab Open University and King Abdulaziz University for supporting carrying out this work.

References

[1] Archer, C.J. and G.R. Ricard, Administering registered virtual addresses in a hybrid computing environment including maintaining a cache of ranges of currently registered virtual addresses. 2016, Google Patents.

[2] Anderson, J.L. and T.J. Balph, Memory interface device with processing capability. 1981, Google Patents.

[3] Kim, S. and R. Lu, The Pseudo-Equivalent Groups Approach as an Alternative to Common-Item Equating. ETS Research Report Series, 2018.

[4] Sansyzbaevich, I.S., et al. Development of algorithm flow graph, mealy automaton graph and mathematical models of microprogram control mealy automaton for microprocessor control device. in Control and Communications (SIBCON), 2017 International Siberian Conference on. 2017. IEEE.

[5] Fujioka, Y., M. Kameyama, and M. Lukac. A dynamically reconfigurable VLSI processor with hierarchical structure based on a micropacket transfer scheme. in Information and Digital Technologies (IDT), 2017 International Conference on. 2017. IEEE.

[6] Kaushansky, D., et al., Programmable test instrument. 2017, Google Patents.

[7] Tan, C.J., et al. Review on Firmware. in Proceedings of the International Conference on Imaging, Signal Processing and Communication. 2017. ACM.

[8] Cabillic, G. and J.-P. Lesot, Selective compiling method, device, and corresponding computer program product. 2017, Google Patents.

[9] Wiśniewski, R., Prototyping of Concurrent Control Systems, in Prototyping of Concurrent Control Systems Implemented in FPGA Devices. 2017, Springer. p. 99-116.

[10] Durand, Y., et al. A Programmable Inbound Transfer Processor for Active Messages in Embedded Multicore Systems. in 2017 Euromicro Conference on Digital System Design (DSD). 2017. IEEE.

[11] Maeda, T. and R. Matsubara, Storage apparatus and failure location identifying method. 2017, Google Patents.

[12] 12. Vladimirov, S. and R. Kirichek, The IoT Identification Procedure Based on the Degraded Flash Memory Sector, in Internet of Things, Smart Spaces, and Next Generation Networks and Systems. 2017, Springer. p. 66-74.

[13] Ye, J., A novel ship-borne positive pressure solid phase extraction device to enrich organo chlorinated and pyrethroid pesticides in seawater. Se pu= Chinese journal of chromatography, 2017. 35(9): p. 907-911.

[14] Vasumathi, B. and S. Moorthi, Implementation of hybrid ANN–PSO algorithm on FPGA for harmonic estimation. Engineering Applications of Artificial Intelligence, 2012. 25(3): p. 476-483.

[15] Wiśniewski, R., Modelling of Concurrent Systems in Hardware Languages, in Prototyping of Concurrent Control Systems Implemented in FPGA Devices. 2017, Springer. p. 117-137.

[16] Pearlson, K.E., C.S. Saunders, and D.F. Galletta, Managing and Using Information Systems, Binder Ready Version: A Strategic Approach. 2016: John Wiley & Sons.

[17] Ruiz, P.A.P., B. Kamsu-Foguem, and D. Noyes, Knowledge reuse integrating the collaboration from experts in industrial maintenance management. Knowledge-Based Systems, 2013. 50: p. 171-186.

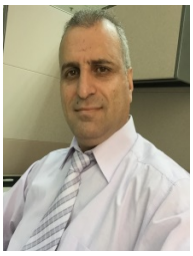
[18] Han, Y.Y., et al., Unexpected increased mortality after implementation of a commercially sold computerized physician order entry system. Pediatrics, 2005. 116(6): p. 1506-1512.

[19] Jagadish, H., et al., Big data and its technical challenges. Communications of the ACM, 2014. 57(7): p. 86-94.

[20] Rafi, D.M., et al. Benefits and limitations of automated software testing: Systematic literature review and practitioner survey. in Proceedings of the 7th International Workshop on Automation of Software Test. 2012. IEEE Press.

[21] Al-Rababah, A. and N. Hani. Component linked based system. in Modern Problems of Radio Engineering, Telecommunications and Computer Science, 2004. Proceedings of the International Conference. 2004. IEEE.

[22] Rodríguez, P., et al., Continuous deployment of software intensive products and services: A systematic mapping study. Journal of Systems and Software, 2017. 123: p. 263-291.
[23] Taylor, S.J., R. Bogdan, and M. DeVault, Introduction to qualitative research methods: A guidebook and resource. 2015: John Wiley & Sons.
[24] Ciccozzi, F., et al., Model-Driven Engineering for Mission-Critical IoT Systems. IEEE Software, 2017. 34(1): p. 46-53.
[25] AlRababah, A.A., A new model of information systems efficiency based on key performance indicator (KPI). management, 2017. 4: p. 8.
[26] Al Ofeishat, H.A. and A.A. Al-Rababah, Real-time programming platforms in the mainstream environments. IJCSNS, 2009. 9(1): p. 197.
[27] Choi, J. and R.A. Rutenbar, Video-rate stereo matching using Markov random field TRW-S inference on a hybrid CPU+ FPGA computing platform. IEEE Transactions on Circuits and Systems for Video Technology, 2016. 26(2): p. 385-398.



Ahmad AbdulQadir Al Rababah received Phd degree in 1998 in computer Engineering, now he is an associate professor at king Abdulaziz university(KSA), he has around 20 experience years of teaching and research in different fields of computing technology and engineering, his research interest areas are: information systems, software engineering, artificial intelligence and others.

Dr. Bandar Ali Alghamdi, holds a PhD from Universite de Reims Champagne-Ardenne in 2015, Reims, France , the M.Sc. degree in Information Technology from De Montfort University, Leicester, United Kingdom, in 2008 and the B.Cs. degree in Computer Sciences from the University of King Abdul-Aziz University, Jeddah, Saudi Arabia, in 2003. Currently he is a Head of Faculty of Computer Studies at Arab Open University, Jeddah, KSA. His research interests are Sensor Networks, Distributed Systems, eHealth Systems, Networking, Testing, Verification, Software Engineering and Real-Time Systems. He has multiple publications in national and international sources.