

Trust Analysis of Link State Network Routing

Dijiang Huang * Deep Medhi * Cory Beard * Lein Harn *

Abstract

Network routing security has received more attention recently. But there are no good design guidelines on how to construct secure network routing domains. There are also no proper evaluation methods to validate the many proposed secure routing frameworks. We analyze network routing security issues via a new approach: trust relations among network routers. Based on the presented trust models for link state routing, we analyze network routing survivability issues. Then we outline the research directions to build secure network routing.

1 Introduction

With recent development of attacking techniques, network routing-based attack has become more common and the attack consequence can be more serious than other traditional network attacks [3]. Very few researchers have been focusing on trust analysis of internetwork routing. We bring up the research issues on the trust relationship among network routers. This research proposes a design guideline from a new perspective to develop a secure network routing protocol and further to design a more robust secure network routing framework.

The paper is arranged as follows: Section 2 presents the trust characteristics of network routing and presents the fundamental analysis tools used by following sections. Section 3 presents our trust relation analysis of a link state routing protocol and survivability analytical results. Finally, in Section 4, we present the outline of our proposal for a secure network routing framework.

2 Trust characteristics in network routing

In this section we discuss trust characteristics and the basic trust elements for network routing.

*School of Computing and Engineering, University of Missouri–Kansas City, Kansas City, MO 64110, USA.

2.1 Trust entities

We assume the communication links are well protected. And our focus is the trust relationships among network routers. And our trust framework is used to regulate the operational roles among network routers. Thus, we define the network routers as trust entities.

2.2 Trust Relations among Network Routers

To develop our trust theory, we propose a new presentation method to define trust relations among network routers:

Definition 1 We use $A\{f : \rightarrow\}B$ to represent the trust relations between two trust entities A and B under some constraint f . It is read “ A trusts B under constraint f ”.

The properties of trust relations are listed as follows:

1. The trust relation $\{f : \rightarrow\}$ is one-way, thus $A\{f : \rightarrow\}B \neq B\{f : \rightarrow\}A$. And we use $A\{f : \rightleftarrows\}B$ to represent that the trust relation between A and B is mutually equal (can also be written as $B\{f : \rightleftarrows\}A$).
2. The constraint f over two trust entities A and B is a set of conditions which include:
 - (a) \subset, \subseteq, \cap : specify the information possession relation between A and B . If information possessed by A and B fulfil the condition $\text{info}(A) \subset \text{info}(B)$ or $\text{info}(A) \subseteq \text{info}(B)$, we denote it as $f_{\{\subset, \subseteq\}}$ or $f_{\{\subseteq, \subset\}}$. When $\text{info}(A)$ and $\text{info}(B)$ do not include each other and $\text{info}(A) \cap \text{info}(B) \neq \phi$, we present the intersection between A and B as $f_{\{\cap, \cdot\}}$.
 - (b) \prec, \preceq : specify the information delivery relation between A and B . If there exists multiple communication channels between A and B , we denote it as $f_{\{\prec, \cdot\}}$; if there exists only one communication channel between A and B , we denote it as $f_{\{\preceq, \cdot\}}$.
 - (c) \approx, \cong : specify the information validation (integrity and authenticity) relations between A and B . If information from B can be verified via other intermediate nodes we denote it as $f_{\{\cdot, \approx\}}$; if information from B can be verified from the information origin source B , we denote it as $f_{\{\cdot, \cong\}}$.

When the conditions do not fulfil the above three types, we use ϕ instead. And we use Θ to represent a set of conditional options.

3. The trust is transferable under constraint f . Such that, if $A\{f : \rightarrow\}B$ and $B\{f : \rightarrow\}C$, then $A\{f : \rightarrow\}C$. Note that the transition occurs only when both trust conditions f are equal.

For example, the trust relation between an OSPF router A and its area border router B can be specified as $A\{f_{\{\subset, \prec, \approx\}} : \rightarrow\}B$. The trust relation is defined based on the facts: $\text{info}(A) \subset \text{info}(B)$, due to flooding and routing

Table 1: Security Mechanisms

Methods		Label	Description
Authentication (A)	Packet	PA_H^\dagger	Hop by hop authentication
	Level	PA_E^\ddagger	End to end authentication
	Information	IA_H^ℓ	Hop by hop authentication
	Level	IA_E^\ddagger	End to end authentication
Confidentiality (C)		CP^\S	For the whole packet
		CI^\ddagger	For the information within the packet

[†]: OSPFv2 RFC2328 and OSPFv3 tentative Internet draft. [‡]:Have not yet proposed.

[§]: OSPF extension RFC2154. ^ℓ: Proposed by Huang et al [2].

information aggregation at B , B knows more information than A ; there are multiple communication channels over which A can receive the information from B ; the routing information received from B is authenticated by a symmetric key shared by all the routers within that area.

2.2.1 Trust validation

The validation of trust can be done via both non-cryptography based and cryptography based methods. First, via a non-cryptography based method, checksum, sequence number, and age are used to validate the routing packet. The trust is secured by network environment, but not by network routing protocols or any cryptographic methods. These configurations are fine when running the routing protocol in a very secure network environment, and move the security management overhead outside of network routing processes.

Another validation type is the cryptography based method, such as authentication and confidentiality, which imbeds cryptography into network routing protocols. Table 1 lists two cryptographic schemes that are described in the literature, including those that have found a place in protocol standards. The two main cryptographic countermeasures that have been suggested for routing protocols are authentication and confidentiality.

The above two types of cryptographic methods can provide protection at the Packet Level or Information Level (we call these two types of data origin authentication as PA and IA respectively). By PA we mean the authentication is processed for a routing update packet or an IP packet that contains the routing update as payload. IA provides protection for each and every piece of routing information carried within a routing update packet. Besides PA and IA, there are two more important concepts we need to introduce into our discussion; they are *hop by hop* (HBH) and *end to end* (ETE). HBH means that the generation and verification of authentication code is performed by every forwarding router. ETE means that the generation of authentication code is performed only at the source; all the forwarding routers and termination routers are part of the system, and they only perform verification. We analyze the combinations between PA, IA and HBH and ETE. For brevity, we identify each mechanism with a label; this is noted in Table 1. From a trust point of view, the HBH needs to set up a trust chain along with the routing information propagation path,

and the ETE is the end-to-end trust relation (every receiver belongs to the end system).

IA_E and IA_H are required to provide information level protection. OSPF with digital signatures [6] is an example of IA_E , while the double authentication scheme [2] is an example of IA_H .

For confidentiality too, we differentiate between packet level and information level, which is shown in Table 1. OSPF running over IPsec [1] is an example of providing C_P , which provides confidentiality for IP payload. Providing confidentiality for each LSA individually is represented by C_I , which has not been proposed in literature.

3 Trust Analysis of Link State Routing

The *open shortest path first* protocol (OSPF) [4] is the most popular link state routing protocol. Based on it, we formulate a simple link state routing model to identify the security issues we will address in this paper.

Within a link state routing domain, each router originates the link state information for the link that has the direct connection with the router and floods. The neighbors will forward the link state information (with tiny modification) to their neighbors except the information incoming link. This flooding procedure will guarantee that each router has the same link state database. Thus each router has the same view of the network. The granularity of routing information in a link state routing protocol is at the level of the link state of a router's interface. This information is called the *link state advertisement* (LSA). During flooding, multiple LSAs can be encapsulated within a single *link state updates* (LSU) routing packet.

The communication security is related to the transmission, reception, and processing of routing data (LSAs and LSUs). Note that all data security related issues we discussed in this paper are based on ROUTING DATA (not user data) and we focus on the communication security aspect of the link-state routing protocol.

3.1 Dominating Factor

After an attacker hacks into the system and occupies a network device (e.g., a router), he can utilize the network routing platform and controlled system resource to deploy attacks. The network failure caused by this type of insider attack is called a Byzantine failure. An attacker can utilize the network control plane, i.e. routing, to deploy more efficient attacks to cause wide area network turbulence or to intercept critical data traffic. Moreover, it is hard to locate Byzantine failures as compared to physical network failures, because the attackers behave like normal routers and the attackers always try to hide their locations and make the network suffer longer.

Based on attack consequences, we classify the Byzantine failure into two types:

Type-I Information failure: the attacks are targeted at deriving network resource allocation information.

Type-II Operation failure: the attacks are targeted at compromising or misleading network operations.

When an attacker hacks into a network router, we call the router a subverted router. As a result, we assume an attacker takes over the router and usurps all the knowledge the subverted router has. To analyze *Type-I* failure, we use \mathcal{P} to represent the overall information of a link state routing domain, \mathcal{S}_{r_i} represents the information known by a router r_i . Thus, we have equation:

$$\mathcal{L}_{r_i} = \frac{|\mathcal{S}_{r_i}|}{|\mathcal{P}|} \quad (1)$$

where, \mathcal{L}_{r_i} represents the proportional information router r_i has, where there are n routers within the link state routing domain, $i = 1, \dots, n$ and $\mathcal{P} = (\mathcal{S}_{r_1} \cup \dots \cup \mathcal{S}_{r_n})$. We call \mathcal{L}_{r_i} as the *dominating factor* of router r_i . We define the information survivability as Γ , which represents the proportion of safe information, i.e.

$$\Gamma = \sum_i^{good} \mathcal{L}_{r_i} \quad (2)$$

where r_i is a good router. If we consider that each router has equal probability to become a subverted router, obviously, $\mathcal{L}_{r_1} = \dots = \mathcal{L}_{r_n}$ is the condition to minimize the variance $V_k(\Gamma)$ of k subverted routers, where $k < n$. The condition $\mathcal{L}_{r_1} = \dots = \mathcal{L}_{r_n}$ specifies that the survivability is router independent.

The analysis based on *Type-II* failure is similar to the analysis of *Type-I* failure. We assume the consequence of failure is the incidence of the overall network, i.e. the proportional number of routers that recognize the network system resource. This is based on the assumption that a subverted router can compromise or mislead other routers based on known network system resources. Thus, for *Type-II* failure, we still can use the survivability Γ defined in the analysis of *Type-I* failure.

3.2 The Trust Model of Link State Routing

In link state network routing, the edge of the network is delimited by the area border and AS (*autonomous system*) boundary. Within an AS, there are multiple areas, and the multiple areas are connected via area 0 (backbone area) to each other and outside of the AS. We classify routers into three groups: the routers within an area (intra-area router r_a); area border router (inter-area router r_b); and AS boundary router r_A , which can be either an intra-area or an inter-area router.

Proposition 1 *We have discussed the current link state routing hierarchy structure (delimited by ASs and areas). We also have presented the*

cryptographic protection summarized in Table 1. We assume there are multiple communication channels between any communication pair (the subverted router cannot partition the network) and the strongest authentication scheme (IA_E) is employed. In our trust presentations, r_a and r_b are in the same area. The trust relations among routers within a link state routing domain are shown as the following:

$$r_a\{f_{\{C, \prec, \cong\}} \rightarrow\}r_b \text{ and } r_b\{f_{\{D, \prec, \cong\}} \rightarrow\}r_a \quad (3)$$

$$r_a\{f_{\{C, \prec, \cong\}} \rightleftarrows\}r'_a \quad (4)$$

$$r_b\{f_{\{C, \prec, \cong\}} \rightleftarrows\}r'_b \text{ or } r_b\{f_{\{area_0, \prec, \cong\}} \rightleftarrows\}r''_b \quad (5)$$

$$r_b\{f_{\{\Theta_1, \prec, \cong\}} \rightleftarrows\}r_A \quad (6)$$

$$r_A\{f_{\{\Theta_2, \prec, \cong\}} \rightleftarrows\}r'_A \quad (7)$$

$$r_a\{f_{\{C, \prec, \cong\}} \rightarrow\}r'_A \text{ or } r_a\{f_{\{AS-info, \prec, \cong\}} \rightarrow\}r''_A \quad (8)$$

$$r'_A\{f_{\{D, \prec, \cong\}} \rightarrow\}r_a \text{ or } r''_A\{f_{\{AS-info, \phi, \phi\}} \rightarrow\}r_a \quad (9)$$

Proof: The following proofs are based on the propagation range of a particular LSA that are generated by a router and the notations defined in Section 2.2 and Section 3.1. Our link state routing analysis model is based on the standard of OSPFv2 [4]. In OSPFv2, 5 types of LSAs are defined. Among them, router LSA, network LSA and summary LSA (type 3 and type 4) are flooded within a particular area and AS-external LSA is flooded over the entire AS. Area border router r_b has an aggregation function to propagate information from outside of an area to the inside. AS border router r_A has an aggregation function to propagate information from outside of an AS to inside.

First, we discuss the second and the third elements of condition f . We assume there are multiple communication channels between any communication pair (the subverted router can not partition the network) and the strongest authentication scheme (IA_E) is employed. These assumptions guarantee that the flooded routing information will be received by every router within its area and the routing protocol is protected by strong authentication scheme. Then, we can infer that forging routing information from any intermediate forwarding router is impossible. Thus, in Equation 3 to Equation 8, all routers in the position B of trust presentation ($A\{f_{\{.,.\}} \rightarrow\}B$) flood the routing information to their areas or AS. A can receive the routing information from at least one communication channel and the routing information is authenticated via strong authentication scheme IA_E . Therefore, we conclude the trust condition from Equation 3 to Equation 8 is $f_{\{.,.\}} \rightarrow$. The exception is the trust presentation of Equation 9. The AS boundary router r_A can be an intra-area router (r'_A) or inter-area router (r''_A). If r'_A and r_a are located within the same area, r_a floods routing information can be reached by r'_A . Thus, we use $f_{\{.,.\}} \rightarrow$ to represent the trust relation from r'_A to r_a . If r''_A and r_a are located within different areas, routing information flooded by r_a would not reach r_A directly. Thus, we use $f_{\{.,\phi,\phi\}} \rightarrow$ to represent the trust relation from r''_A to r_a .

The following discussion is focused on the first element of condition f .

Proof of Equation (3): r_b and r_a locate within the same area. r_b will aggregate routing information from outside of an area to inside of an area. Thus, $\text{info}(r_a) \subset \text{info}(r_b)$ and $\mathcal{S}_{r_a} \subset \mathcal{S}_{r_b}$.

Proof of Equation (4): r_a and r'_a locate within the same area. Link state routing protocol floods LSA within an area or an AS. Thus, $\text{info}(r_a) = \text{info}(r'_a)$, $\mathcal{S}_{r_a} \subseteq \mathcal{S}_{r'_a}$ and the same in the reverse direction.

Proof of Equation (5): due to flooding, when r_b and r'_b belong to same area (both area 0 and intra-area), $\text{info}(r_b) = \text{info}(r'_b)$, $\mathcal{S}_{r_b} \subseteq \mathcal{S}_{r'_b}$ and the same in the reverse direction. When r_b and r''_b only belong to the same area 0, $\text{info}(r_b) \cap \text{info}(r''_b) = \text{info}(\text{area } 0)$, $\text{info}(r_b) \neq \text{info}(r''_b)$, $\mathcal{S}_{r_b} \cap \mathcal{S}_{r''_b} = \{\overset{\cap}{\text{area } 0}\}$.

Proof of Equation (6): the routing information possessed by router r_b and r_A are different. They both aggregate routing information and propagate to different areas. Case 1: if r_b and r_A are located within the same intra-area and r_A is not the area border router, thus $\mathcal{S}_{r_b} \cap \mathcal{S}_{r_A} = \{\overset{\cap}{\text{intra-area}}\} \cup \{\overset{\cap}{\text{AS-info}}\}$. Case 2: if r_b and r_A are located within the same intra-area as well as inter-area (area 0), thus $\mathcal{S}_{r_b} \subset \mathcal{S}_{r_A}$. Case 3: if r_b and r_A are located within different intra-area and r_A is not an area border router, thus $\mathcal{S}_{r_b} \cap \mathcal{S}_{r_A} = \{\overset{\cap}{\text{AS-info}}\}$. Case 4: if r_b and r_A are located within different intra-area and also within area 0, thus $\mathcal{S}_{r_b} \cap \mathcal{S}_{r_A} = \{\overset{\cap}{\text{area } 0}\} \cup \{\overset{\cap}{\text{AS-info}}\}$. In summary, $\Theta_1 = \{\{\overset{\cap}{\text{intra-area}}\} \cup \{\overset{\cap}{\text{AS-info}}\} | \mathcal{S}_{r_b} | \{\overset{\cap}{\text{AS-info}}\} | \{\{\overset{\cap}{\text{area } 0}\} \cup \{\overset{\cap}{\text{AS-info}}\}\}$ in the presented four cases, where “|” is “or” operator. Similarly, we can prove that the reverse trust relation between r_b and r_A is the same.

Proof of Equation (7): Case 1: if r_A and r'_A are located within the same intra-area, $\mathcal{S}_{r_A} \cap \mathcal{S}_{r'_A} = \{\overset{\cap}{\text{intra-area}}\} \cup \{\overset{\cap}{\text{AS-info}}\}$. Case 2: if r_A and r'_A are located within different intra-area and at least one of them does not belong to area 0, $\mathcal{S}_{r_A} \cap \mathcal{S}_{r'_A} = \{\overset{\cap}{\text{AS-info}}\}$. Case 3: if r_A and r'_A are located within different intra-area and both of them belong to area 0, $\mathcal{S}_{r_A} \cap \mathcal{S}_{r'_A} = \{\overset{\cap}{\text{area } 0}\} \cup \{\overset{\cap}{\text{AS-info}}\}$. In summary, $\Theta_2 = \{\{\overset{\cap}{\text{intra-area}}\} \cup \{\overset{\cap}{\text{AS-info}}\} | \{\overset{\cap}{\text{AS-info}}\} | \{\{\overset{\cap}{\text{area } 0}\} \cup \{\overset{\cap}{\text{AS-info}}\}\}$

Proof of Equation (8): Case 1: if r_a and r'_A belong to the same intra-area, $\mathcal{S}_{r_a} \subset \mathcal{S}_{r'_A}$. Case 2: if r_a and r''_A belong to different intra-area, $\mathcal{S}_{r_a} \cap \mathcal{S}_{r''_A} = \{\overset{\cap}{\text{AS-info}}\}$.

Proof of Equation (9): the proof is the same as the proof of Equation 8. ■

3.3 Upper Bound and Lower Bound Analysis of Link State Routing Survivability

In this section, we analyze the survivability of link state routing based on the dominating factor (\mathcal{L}) presented in Section 3.1 and Proposition 1 presented in Section 3.2.

A link state routing domain contains n routers ($n \geq 2$), and there are $k + 1$ areas within the link state routing domain (k intra-areas and one area 0 – backbone), thus $n = \sum_{i=1}^k n_i$. Our upper bound and lower bound analysis is given based on the following assumptions:

1. We discuss the circumstance that only one subverted router exists within the link state routing domain and each router can be subverted with equal probability.
2. Trust is built between any possible pair of originator (or forwarder) and receiver.
3. At least one intra-area (non-area 0) is constructed. Area 0 is constructed by all intra-area border routers. An intra-area contains at least two routers and any intra-area contains at most $\frac{n}{2}$ routers, thus $1 \leq k \leq \frac{n}{2}$, where k is the number of intra-areas within the link state routing domain (do not include area 0) and n is the total number of routers within the link state routing domain.

Assumption 1 implies that each intra-area router r_a can be subverted with equal probability, then we require $n_1 = \dots = n_k$ to minmax the dominating factor \mathcal{L}_{r_i} of all routers ($r_i, i = 1, 2, \dots, n$).

We note that a router sends routing information within an area or AS. Due to flooding, the routing information can be received by all the routers within that area or AS. We infer that the trust is implicitly built between any possible pair of originator (or forwarder) and receiver (specified in assumption 2). Hence, we use the number of paths for every pair of routers (restricted by one path per pair) to represent the number of one-to-one trust relations among routers. This assumption is valid, since we define the trust is one-to-one relation; if there exists at least one connected path between two routers, there will be ONE trust relation between these two routers. For example, if there are n_i routers within an area and they create a connected graph with n_i nodes, there will be $\binom{n_i}{2}$ trust relations within that area. We use italic *path* to represent a trust relation in the rest of this paper.

To simplify our trust analysis, from assumption 3, an area has minimal 2 routers (1 *path*) and maximal $\frac{n}{2}$ routers ($\binom{\frac{n}{2}}{2} = \frac{n(n-2)}{8}$ *paths*).

3.3.1 Subverted router r_a

If r_a is compromised, from Equation 4, we know all the information within r_a 's area is compromised. From Equation 3, we know r_a knows the destinations of the inter-area networks and AS boundary routers and corresponding explicit routes to the area border routers. The knowledge of explicit routes is limited within its area. The Equation 8 shows that the information shared from r_A to r_a is the aggregated routes information to outsider of AS via r_A . If r_A is an intra-area router or area border router located within the same area as r_a , the shared information will be the explicit routes within the area; if r_A and r_a are located within different areas, the shared information will be the paths to the r_A on which area border routers r_b . In a summary, the explicit routes information known by r_a is bounded by its area border. If r_a is an intra-area router of area i and \mathcal{S}_{r_a} represents the total number of trust relations (*paths*¹) in area i that is

¹Based on assumption 2, each pairwise trust relation is represented by a *path* and the *path* is limited by one *path* per pair nodes.

known by router r_a , we conclude $\mathcal{S}_{r_a} = \bigcup_{\text{area } i} (\text{all paths})$. Bounded by the area border, we present all the *paths* within a link state routing domain as $\mathcal{P} = \bigcup_{\text{area } i=1}^k (\text{all paths}) \cup \{\text{all paths in area 0}\}$. Thus we have the upper bound of dominating factor \mathcal{L}_{r_a} :

$$\begin{aligned} \mathcal{L}_{r_a} &= \frac{|\mathcal{S}_{r_a}|}{|\mathcal{P}|} = \frac{|\bigcup_{\text{area } i} (\text{all paths})|}{|\bigcup_{i=0} (\text{all paths})|} < \frac{|\bigcup_{\text{area } i} (\text{all paths})|}{|\bigcup_{i=1} (\text{all paths})|} \\ &< \frac{1}{k} \quad (1 \leq k \leq \frac{n}{2}) \quad (\text{using assumption 1}) \end{aligned} \quad (10)$$

To analysis the lower bound of dominating factor of router r_a , we assume there are k intra-areas and there are k area border routers to minimize the number of *paths* in area 0, i.e. $\binom{k}{2}$. Due to assumption 1, there are $\frac{n}{k}$ routers in each intra-area. Thus, the number of *paths* in each intra-area is $\binom{\frac{n}{k}}{2}$. Therefore, the lower bound of \mathcal{L}_{r_a} is shown as follows:

$$\begin{aligned} \mathcal{L}_{r_a} &= \frac{|\mathcal{S}_{r_a}|}{|\mathcal{P}|} = \frac{|\bigcup_{\text{area } i} (\text{all paths})|}{|\bigcup_{i=0} (\text{all paths})|} = \frac{\binom{\frac{n}{k}}{2}}{k\binom{\frac{n}{k}}{2} + \binom{k}{2}} \\ &= \frac{1}{k + \frac{k^4 - k^3}{n^2 - nk}} \geq \frac{8}{n^2 + 2n} \quad (\text{when } k = \frac{n}{2}) \end{aligned} \quad (11)$$

3.3.2 Subverted router r_b

When r_b is compromised, from Equation 3, we know all the information within r_b 's intra-area is compromised. From Equation 5, we know all the information within backbone (area 0) is compromised. Thus, if r_b is a subverted area border router for s areas (exclude area 0), where $s \leq k$, we conclude $\mathcal{S}_{r_b} = \bigcup_{i=1}^s (\text{all paths in area } i)$.

To analyze the upper bound, we consider the extreme case that every router is an area border router. Thus area 0 will have $\binom{n}{2}$ *paths*. We have the upper bound of dominating factor \mathcal{L}_{r_b} :

$$\begin{aligned} \mathcal{L}_{r_b} &= \frac{|\bigcup_{i=0}^s (\text{all paths in area } i)|}{|\bigcup_{i=0} (\text{all paths in area } i)|} = \frac{\binom{n}{2} + s\binom{\frac{n}{k}}{2}}{\binom{n}{2} + k\binom{\frac{n}{k}}{2}} = \frac{(n^2 - n) - \frac{sn}{k} + \frac{sn^2}{k^2}}{n^2 - 2n + \frac{n^2}{k}} \\ &\leq \frac{n^4 - n^3 + 2sn^2}{n^4} \quad (\text{when } k = \frac{n}{2}, s \leq k) \end{aligned} \quad (12)$$

To analyze the lower bound, we consider the extreme case that each area contains only 1 inter-area router, and all other routers are intra-area routers. The area border routers construct the backbone (area 0) with k area border routers ($\binom{k}{2}$ paths). A router r_b can be an area border router for maximally s areas, where $s \leq k$. Therefore, we have the lower bound of dominating factor \mathcal{L}_{r_b} :

$$\begin{aligned} \mathcal{L}_{r_b} &= \frac{|\bigcup_{i=0}^s (\text{all paths in area } i)|}{k} = \frac{\binom{k}{2} + s\binom{\frac{n}{2}}{2}}{\binom{k}{2} + k\binom{\frac{n}{2}}{2}} = \frac{k^4 - k^3 - snk + sn^2}{k^4 - k^3 - nk^2 + n^2k} \\ &\geq \frac{k^4 - k^3 + n^2 - nk}{k^4 - k^3 + kn^2 - k^2n} \geq \frac{n^4 - 2n^3 + 8n^2}{n^4 + 2n^3} \quad (\text{when } k = \frac{n}{2}) \end{aligned} \quad (13)$$

3.3.3 Subverted router r_A

When a r_A is compromised, from Equation 6, 7 and Equation 9, we know the maximum number of trusted one-to-one relations that will be compromised by a subverted r_A is $\{\text{area } i\} \cup \{\text{area } 0\} \cup \{AS\text{-info}\}$ and the minimum number of trusted one-to-one relations that will be compromised by a subverted r_A is $\{\text{area } i\} \cup \{AS\text{-info}\}$.

To analyze the upper bound, we consider the extreme case that every router is an area border router, which belongs to area 0. Every r_A is an area border router. The upper bound analysis is the same as the upper bound analysis of r_b . Thus we have the upper bound of dominating factor \mathcal{L}_{r_A} :

$$\mathcal{L}_{r_A} \leq \frac{n^4 - n^3 + 2sn^2}{n^4} \quad (k = \frac{n}{2}, s \leq k) \quad (14)$$

Similarly, the lower bound analysis of a subverted router r_A is also the same as the lower bound analysis of a subverted router r_b . Therefore, we have the lower bound of dominating factor \mathcal{L}_{r_A} :

$$\mathcal{L}_{r_A} \geq \frac{n^4 - 2n^3 + 8n^2}{n^4 + 2n^3} \quad (s = 1, k = \frac{n}{2}) \quad (15)$$

4 Conclusion

The minimal scale of trust relation is a link state routing area. Within an area, a router will share all of its network resources information with other routers. This is the trust property of current link state routing. Without changing the minimal scale of trust relation or current link state routing, we cannot achieve better survivability due to our study in Section 3.

Our solution is to achieve better information survivability without changing current link state routing administrative domains. In the mean time, we require minimal changes in the procedure of link state routing protocols.

4.1 Our Proposal and Future Work

Using confidentiality provides a natural way for us to divide the routing domain into multiple small size *trust domains* (TDs). Each TD represents a subset of network resource (a path, several paths or a tree). In this way, as long as the $\text{info}(\text{TD}) \subset \text{info}(\text{an area})$, we can achieve better survivability related to the equations presented in Section 3. The philosophy behind this is that a router needs to know only the necessary routes going through it. Therefore, we refer to the cryptographic method C_I presented in Table 1. C_I provides confidentiality for the routers that have built trust within their TD. Thus, multiple TDs can be differentiated by providing different levels of confidentiality. In this way, we can reduce the upper bound presented by Equation 10, Equation 12 and Equation 14.

Trust is built among routers, and it is set up by the shared keys among routers or key certificates provided by some key certificate servers. The trust validation is processed through cryptographic operations, such as authentication and encryption/decryption. Thus, key management plays an indispensable role in determining the trust relations among routers. A flexible and scalable group keying scheme is needed. Due to frequent routing information exchange, the use of a shared key scheme is desired in order to minimize computational overhead. The group keying scheme is flexible to support group/subgroup communication to reduce overhead caused by subgroup formation process. It is desired that a router be able to generate the corresponding subgroup key based on the trust token (router ID, domain ID, etc.). There are many candidates for key management schemes; two good surveys can be found in [7] and [5].

To carry the additional information such as the hidden resource information in the link-state advertisement, extensions to routing protocol messages need to be deployed. We exploit this capability of the OSPF Opaque LSA extension (RFC 2370).

References

- [1] M. Gupta, N. Melam, "Authentication/Confidentiality for OSPFv3", Internet draft, November, 2002.
- [2] D. Huang, A. Sinha, D. Medhi, A Double Authentication Scheme To Detect Impersonation Attack In Link State Routing Protocols, IEEE International Conference on Communications (ICC'03), May 2003.
- [3] K. J. Houle, G. M. Weaver, N. Long and R. Thomas "Trends in Denial of Service Attack Technology", *CERT® Coordination Center*, 2001.
- [4] J. Moy, "OSPF version 2", RFC 2328, April 1998.
- [5] M. J. Moyer, J. R. Rao and P. Rohatgi, "A Survey of Security Issues in Multicast Communications". *IEEE Network*, November/December, 1999.
- [6] S. Murphy, M. Badger and W. Wellington, "OSPF with Digital Signatures", RFC 2154, June 1997.
- [7] D. R. Stinson, "On Some Methods for Unconditionally Secure Key Distribution and Broadcast Encryption". *Designs, Codes and Cryptography*, 12, pp. 215-243, 1997.